

**MORGAN & MORGAN
COMPLEX LITIGATION GROUP**
John A. Yanchunis (Admitted Pro Hac Vice)
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
Telephone: 813/223-5505
813/223-5402 (fax)
jyanchunis@ForThePeople.com

**CASEY GERRY SCHENK
FRANCAVILLA BLATT & PENFIELD
LLP**
Gayle M. Blatt, SBN 122048
110 Laurel Street
San Diego, CA 92101
Telephone: 619/238-1811
619/544-9232 (fax)
gmb@cglaw.com

MILBERG LLP
Ariana J. Tadler (Admitted Pro Hac Vice)
One Pennsylvania Plaza
New York, NY 10119
Telephone: 212/594-5300
212/868-1229 (fax)
atadler@milberg.com

**ROBBINS GELLER RUDMAN
& DOWD LLP**
Stuart A. Davidson (Admitted Pro Hac
Vice)
120 East Palmetto Park Road, Suite 500
Boca Raton, FL 33432
Telephone: 561/750-3000
561/750-3364 (fax)
sdavidson@rgrdlaw.com

**LOCKRIDGE GRINDAL NAUEN
P.L.L.P.**
Karen Hanson Riebel (Admitted Pro Hac
Vice)
100 Washington Ave. South, Suite 2200
Minneapolis, MN 55401
Telephone: 612/339-6900
612/339-0981 (fax)
khriebel@locklaw.com

Attorneys for Plaintiffs and the Class

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION**

IN RE: YAHOO! INC. CUSTOMER DATA
SECURITY BREACH LITIGATION

CASE NO. 16-MD-02752-LHK

**FIRST AMENDED CONSOLIDATED
CLASS ACTION COMPLAINT**

JURY TRIAL DEMANDED

TABLE OF CONTENTS

I.	SUMMARY OF THE CASE.....	1
II.	JURISDICTION AND VENUE	6
III.	PARTIES	7
A.	Class Representatives Who Signed up for Yahoo Services in the United States	7
B.	Class Representatives for the Israel Class	11
C.	Class Representative for the Small Business Users Class	12
D.	Class Representative for the Paid Users Class.....	14
E.	Defendants	15
IV.	FACTUAL BACKGROUND.....	16
A.	Yahoo Collects and Stores PII for its Own Financial Gain	16
B.	Yahoo’s Small Business Customers Depended on Defendants’ PII Security Practices	19
C.	PII is Very Valuable on the Black Market.....	22
D.	Yahoo Turns a Blind Eye to Gaping Holes in Its Security, Refusing to Upgrade After Repeated Intrusions and Negative Assessments.....	25
E.	Yahoo’s Inadequate Data Security Allows the Massive Breach of 1 Billion User Accounts in 2013, Which Yahoo Then Fails to Disclose	31
F.	Yahoo’s Security Is Breached Again and Again—in 2014, 2015, and 2016—Yet Yahoo Still Does Not Alert Its Users	34
G.	Yahoo Reveals the 2014 Breach Years After It Happened.....	43
H.	More Than Three Years After the Fact, Yahoo Finally Acknowledges the 2013 Breach	46
I.	Despite All of This, Yahoo Still Waits to Notify Users Affected by the Forged Cookie Breach	48
J.	The Full Extent of the Fallout from the Breaches is Not Yet Known ..	50
V.	CLASS ACTION ALLEGATIONS	55
VI.	CHOICE OF LAW	61
VII.	CLAIMS ALLEGED ON BEHALF OF ALL CLASSES.....	63
	First Claim for Relief: Violation of California’s Unfair Competition Law	

	(“UCL”) – Unlawful Business Practice	63
1		
2	Second Claim for Relief: Violation of California’s Unfair Competition Law (“UCL”) – Unfair Business Practice.....	66
3		
4	Third Claim for Relief: Deceit by Concealment — Cal. Civil Code §§ 1709, 1710.....	70
5		
6	Fourth Claim for Relief: Negligence	72
7		
8	Fifth Claim for Relief: Breach of Contract	74
9		
10	Sixth Claim for Relief: Breach of Implied Contracts	79
11		
12	Seventh Claim for Relief: Breach of the Implied Covenant of Good Faith and Fair Dealing	80
13		
14	Eighth Claim for Relief: Declaratory Relief.....	81
15		
16	VIII. ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE SMALL BUSINESS USERS CLASS ONLY.....	83
17		
18	Ninth Claim for Relief: Violation of California’s Unfair Competition Law (“UCL”) – Fraudulent Business Practice.....	83
19		
20	Tenth Claim for Relief: Misrepresentation	85
21		
22	IX. ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE PAID USERS CLASS ONLY	87
23		
24	Eleventh Claim for Relief: Violation of California’s Consumer Legal Remedies Act (“CLRA”)	87
25		
26	X. ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE CALIFORNIA SUBCLASS ONLY	90
27		
28	Twelfth Claim for Relief: Violation of California’s Customer Records Act – Inadequate Security.....	90
	Thirteenth Claim for Relief: Violation of California’s Customer Records Act – Delayed Notification.....	92
	XI. PRAYER FOR RELIEF	96
	XII. JURY TRIAL DEMANDED.....	97

1 For their First Amended Consolidated Class Action Complaint, Plaintiffs Kimberly
2 Heines, Hashmatullah Essar, Paul Dugas, Matthew Ridolfo, Deana Ridolfo, Yaniv Rivlin,
3 Mali Granot, Brian Neff, and Andrew J. Mortensen, on behalf of themselves and all others
4 similarly situated, allege the following against Defendant Yahoo! Inc. (“Yahoo”),¹ and
5 Plaintiff Brian Neff, on behalf of himself and all others similarly situated, alleges the
6 following against Defendants Yahoo and Aabaco Small Business, LLC (“Aabaco”)
7 (collectively with Yahoo, “Defendants”), based on personal knowledge as to Plaintiffs and
8 Plaintiffs’ own acts and on information and belief as to all other matters based upon, *inter*
9 *alia*, the investigation conducted by and through Plaintiffs’ undersigned counsel:

10 **SUMMARY OF THE CASE**

11 1. Giant information service providers such as Google, Facebook, Microsoft, and
12 Yahoo experience a consistent stream of attacks on their data security. Quickly identifying
13 and documenting those attacks, stopping them, and crafting better security measures to
14 prevent them in the future is a normal, expected part of the business – except in Yahoo’s
15 case. Inexplicably turning a blind eye to this key aspect of its business, Yahoo did not just
16 ignore security holes, it failed to set up the systems necessary to even detect or document
17 them. This practice was long-term. Yahoo’s own documents demonstrate that for nearly the
18 last decade, Yahoo’s systems have been breached again and again and again and that Yahoo
19 in essence did nothing to protect its user data.

20 2. As a telling example, law enforcement notified Yahoo of a potential breach in
21 late 2011. It took Yahoo until January 30, 2012, to retain an outside cybersecurity firm,

22 ¹ In June, 2017, Yahoo’s operating business was acquired by Verizon Communications
23 Inc. (“Verizon”), with Yahoo continuing to exist as a wholly-owned subsidiary of Oath, Inc.,
24 a subsidiary of Verizon. In the event Yahoo is unable to satisfy any judgment entered in this
25 case against it, and a successor entity is the proper defendant, plaintiffs will promptly move
26 under Rule 25(c) to substitute Yahoo’s successor as a proper defendant, which may be done
27 at any time, including after judgment. *See Fed. Ins. Co. v. Laney*, No. C 12-04708 WHA,
28 2013 WL 3597309, at *2 (N.D. Cal. July 12, 2013) (noting that “Rule 25(c) has no time
limit.”); *Zest IP Holdings, LLC v. Implant Direct Mfg, LLC*, No. 10CV0541-GPC-WVG,
2013 WL 1626111, at *2 (S.D. Cal. Apr. 15, 2013) (“Rule 25(c) does not have a time limit,
however, and joinder may occur at any point during litigation, even after judgment has been
rendered.”).

1 Mandiant, to investigate that breach. Even then, Yahoo did not want to investigate too
2 thoroughly, instructing Mandiant not to perform any “Live Response or forensic analysis of
3 any compromised system.”

4 3. Even with the investigative limitations, Mandiant’s resulting report, released
5 to Yahoo on April 20, 2012, was damning: [REDACTED]

6 [REDACTED]

7 [REDACTED]

8 [REDACTED]

9 [REDACTED]

10 [REDACTED]

11 [REDACTED] That alone should have caused Yahoo to start to invest in greater security, [REDACTED]

12 [REDACTED]

13 But, Yahoo did not. Thus, Yahoo was breached again later in 2012, with attackers
14 absconding with private information of more than 450,000 user accounts.

15 4. Yahoo’s sheer recklessness with respect to data security led to predictable
16 results. In September 2016, Yahoo rocked the technology world by disclosing that
17 information was stolen from 500 million user accounts *two years earlier* in the then-largest
18 known data breach in history (the “2014 Breach”). Only two months later, Yahoo again made
19 headlines around the globe when it admitted to an even more massive breach—affecting
20 upwards of 1 billion user accounts—that had occurred *three years* before Yahoo made the
21 admission (the “2013 Breach”).

22 5. In late 2017, the other shoe dropped. Yahoo admitted the 2013 Breach was
23 even larger than originally disclosed—by a magnitude of three. *All three billion* Yahoo
24 accounts then existing were breached in 2013, a fact that Yahoo falsely claims—as detailed
25 herein—took more than four years to discover and disclose.

26 6. Yahoo’s substandard security also permitted third parties to forge cookies,
27 affecting approximately 32 million accounts between 2015 and 2016. Yahoo acknowledged
28 the existence of the Forged Cookie Breach as early as November 2016, buried in the fine

1 print of an SEC filing, but delayed notifying affected consumers for several months. In fact,
2 Yahoo waited until a few months into 2017 to begin notifying Yahoo users that they had
3 been the victims of the “Forged Cookie Breach.”²

4 7. During the 2013 and 2014 Breaches, hackers were able to take the names,
5 email addresses, telephone numbers, birth dates, passwords, and security questions of Yahoo
6 account holders. As a result, the hackers gained access to the contents of *all* breached Yahoo
7 accounts and, thus, any private information contained within users’ emails, calendars, and
8 contacts, including financial communications and records containing credit cards, retail
9 accounts, banking, account passwords, IRS documents, and social security numbers from
10 transactions conducted by email, in addition to other confidential and sensitive information.
11 This compromised data is collectively referred to herein as “Personal Identifying
12 Information” or “PII.”

13 8. Despite the staggering magnitude of these breaches, Yahoo initially claimed
14 that it did not discover the 2014 Breach or 2013 Breach *until 2016*. However, Yahoo’s own
15 internal documents clearly indicate that this claim was and is untrue. In fact, Yahoo—
16 including key members of its legal team— knew about the 2014 Breach, internal code name
17 “Siberia,” *at the time it was occurring*. In an exchange on *November 5, 2014*, Yahoo
18 personnel (Jeff Zingler, Software Development Engineer, and Andrew Rios, Incident
19 Response) discuss a meeting with the legal team about the 2014 Breach:

20	11.5.14, 11:06	Andrew R.	Hey Jeff, are you guys still
21			having the strategy meeting?
22	11.5.14, 11:10	Jeff Z.	ah sorry, Ramses [Martinez]
23			is caught up with Legal. Ill
24			ping you if he gets
25			finished.
26	11.5.14, 11:10	Jeff Z.	Siberia shit.....

27 9. Indeed, although Yahoo’s decision-makers made a conscious and deliberate
28

² The 2013 Breach, 2014 Breach, and Forged Cookie Breach are collectively referred to as the “Yahoo Data Breaches” or “Data Breaches.”

1 decision not to alert any of Yahoo’s customers that their PII had been stolen, they created a
2 “reactionary” press release about the 2014 Breach, to use in the event that it became public
3 before Yahoo wanted to disclose it.

4 10. In its 2016 annual filing with the SEC, Yahoo admitted an independent
5 investigation showed it had “contemporaneous knowledge” of the 2014 Breach, yet failed to
6 “properly investigate[] and analyze[]” the breach, due in part to “failures in communication,
7 management, inquiry and internal reporting” that led to a “lack of proper comprehension and
8 handling” of the 2014 Breach.³ The 10-K provided additional details regarding Yahoo’s
9 failures:

10 Specifically, as of December 2014, the information security team
11 understood that the attacker had exfiltrated copies of user database backup
12 files containing the personal data of Yahoo users but it is unclear whether
13 and to what extent such evidence of exfiltration was effectively
14 communicated and understood outside the information security team.
15 However, the Independent Committee did not conclude that there was an
16 intentional suppression of relevant information.

17 Nonetheless, the Committee found that the relevant legal team had
18 sufficient information to warrant substantial further inquiry in 2014, and
19 they did not sufficiently pursue it. As a result, the 2014 Security Incident
20 was not properly investigated and analyzed at the time, and the Company
21 was not adequately advised with respect to the legal and business risks
22 associated with the 2014 Security Incident. The Independent Committee
23 found that failures in communication, management, inquiry and internal
24 reporting contributed to the lack of proper comprehension and handling of
25 the 2014 Security Incident. The Independent Committee also found that
26 the Audit and Finance Committee and the full Board were not adequately
27 informed of the full severity, risks, and potential impacts of the 2014
28 Security Incident and related matters.⁴

11. Even more astoundingly, Yahoo did not begin to disclose the 2013 Breach—
the one involving all 3 billion accounts—until three years after it happened. Despite the
wealth of evidence of ongoing security breaches and problems, Yahoo claims to have been
totally unaware of this breach until being notified by law enforcement in 2016. Even after

³ Yahoo!, Inc. 2016 Form 10-K (March 1, 2017), p. 47, <https://investor.yahoo.net/secfiling.cfm?filingID=1193125-17-65791&CIK=1011006>.

⁴ *Id.*

1 that, it took nearly another full year for Yahoo to disclose the true extent of the 2013 Breach,
2 tripling its size.

3 12. Restated in simple terms, Yahoo is claiming that in 2013 its data security
4 measures and breach detection measures were so poor that hackers were able to access every
5 single Yahoo account—roughly 3 billion—and exfiltrate users’ PII, and Yahoo never
6 detected it. This is the biggest data breach in history, by far, and Yahoo purports to have
7 known nothing about it until told by someone else. Someone who, unlike Yahoo, was not
8 charged with protecting Yahoo’s stored information.

9 13. To make matters worse, at the time of the 2013 Breach, Yahoo was still using
10 an encryption technology called MD5, which at least five years earlier had been publicly
11 discredited and deemed “cryptographically broken and unsuitable for further use.”⁵ So,
12 identity thieves had three full years of unfettered access to the inadequately-encrypted PII of
13 roughly 3 billion user accounts before Yahoo even began to notify its users that their PII had
14 been compromised.

15 14. Both the scope of these three massive data breaches and Yahoo’s baffling and
16 unlawful delay in notification is unprecedented in the information technology world.

17 15. This First Amended Consolidated Class Action Complaint is filed on behalf of
18 all persons in the United States and Israel, described more fully in the following sections,
19 whose PII was compromised in the 2013, 2014, or Forged Cookie Breaches. The class
20 representatives here have suffered actual harm, including, but not limited to, having false tax
21 returns filed in their name, having credit card accounts fraudulently opened in their names,
22 having fraudulent charges posted to their credit cards and bank accounts, having their
23 government benefits stolen, and having spam and phishing emails sent constantly from their
24 Yahoo addresses. The compromise of the Class members’ PII has also caused the Class
25 members to pay for credit monitoring, account freezes, card and account replacements, and
26

27 ⁵ Joseph Menn, Jim Finkle, & Dustin Volz, INSIGHT-Yahoo security problems a story of too
28 little, too late, CNBC (Dec. 18, 2016, 5:09 PM), <http://www.cnbc.com/2016/12/18/reuters-america-insight-yahoo-security-problems-a-story-of-too-little-too-late.html>.

1 late fees for delayed payments. Class members have devoted and will continue to devote time
2 and energy to recovering stolen funds (where possible), tracking and repairing damage to
3 their credit reports and reputations, and monitoring and protecting their accounts. Plaintiffs
4 and Class members are further damaged as their PII remains in Defendants' possession,
5 without adequate protection, and is also in the hands of those who obtained it for its
6 commercial value, without Plaintiffs' or Class members' consent. Further, members of the
7 Small Business Class and the Paid Users Class have lost the benefit of their bargain and
8 purchased services they otherwise would not have, or paid more for supposedly secure
9 services than they would have, had they known the truth regarding Defendants' inadequate
10 data security.

11 **JURISDICTION AND VENUE**

12 16. This Court has jurisdiction over this action pursuant to the Class Action
13 Fairness Act ("CAFA"), 28 U.S.C. § 1332(d), because the aggregate amount in controversy
14 exceeds \$5,000,000, exclusive of interests and costs, there are more than 100 class members,
15 and at least one class member is a citizen of a state different from Defendants and is a citizen
16 of a foreign state. The Court also has supplemental jurisdiction over the state law claims
17 pursuant to 28 U.S.C. § 1367.

18 17. Venue is proper under 28 U.S.C. § 1391(c) because Defendants are
19 corporations that do business in and are subject to personal jurisdiction in this District. Venue
20 is also proper under 28 U.S.C. § 1391(b) based on the Transfer Order of the Judicial Panel on
21 Multidistrict Litigation, ECF No. 62, and because a substantial part of the events or
22 omissions giving rise to the claims in this action occurred in or emanated from this District,
23 including the decisions made by Yahoo's governance and management personnel that led to
24 the breaches. Further, Yahoo's and Aabaco's terms of service governing users in the United
25 States and Israel provide for California venue for all claims arising out of Plaintiffs'
26 relationship with Yahoo and/or Aabaco.

PARTIES

A. Class Representatives Who Signed up for Yahoo Services in the United States

18. Plaintiff Kimberly Heines is a resident and citizen of Magalia, California. Ms. Heines receives approximately \$1,100 per month from Social Security Disability to meet her essential needs, including food and housing. Plaintiff Heines opened a Yahoo account nearly twenty years ago and used it for all of her online communications, including communications relating to her education, financial aid, employment, banking, healthcare, and personal finances. Plaintiff Heines' Yahoo emails included PII and information relating to her account with Direct Express, the payment service through which she receives her Social Security Disability benefits. On February 4, 2015, Plaintiff Heines discovered that her entire monthly disability allowance had been stolen from her Direct Express account and used to purchase gift cards at Rite Aid (in the amounts of \$513.58 and \$507.10), and Walgreens (in the amount of \$118.00). Plaintiff Heines had her Direct Express card in her possession at the time of the thefts and was away from home caring for a hospitalized relative, more than 600 miles from where the thefts occurred. Because she had no other source of income, the theft put her in an extremely vulnerable and stressful situation in which she literally had to rely on the kindness of strangers to survive for two weeks. Plaintiff Heines is normally very conscientious about paying bills on time but the theft caused her to pay her rent and some utility bills late, which resulted in late fees of more than \$30. Soon after the theft, Ms. Heines started receiving collection calls regarding debts she had not incurred. She also saw unfamiliar debts appearing on her credit report and her credit score suffered as a result. Plaintiff Heines filed a police report and spent over 40 hours talking to the police, the Social Security Administration, Direct Express, RiteAid, Walgreens, and others to have the funds restored to her Direct Express account and deal with other consequences of the data breach, the resulting theft, and the consequences of the theft. In or about September 2016, Plaintiff Heines received an email notice from Yahoo informing her that her Yahoo accounts and PII may have been compromised in the 2014 Breach. In addition to the damages detailed herein,

1 the Yahoo Data Breaches have caused Plaintiff Heines to be at substantial risk for further
2 identity theft.

3 19. Plaintiff Hashmatullah Essar is a resident and citizen of Thornton, Colorado.
4 Mr. Essar is a retail manager for a local bank and handles retail and banking accounts.
5 Approximately 15 years ago, Mr. Essar opened two email accounts with Yahoo. Mr. Essar
6 carefully read the Terms of Service before opening his email accounts and would not have
7 opened them if he had any concerns about the security of Yahoo email. Mr. Essar used his
8 Yahoo email accounts for all of his personal, financial, and business needs. More
9 specifically, Plaintiff Essar transacted business, shopped online, sent personal messages,
10 communicated with his accountant, received bank account statements, applied for jobs,
11 secured a mortgage for his home, and refinanced that mortgage, through his Yahoo e-mail
12 account. Plaintiff Essar first became concerned about the security of his Yahoo email
13 accounts when he received phishing emails from a credit card company purporting to be
14 affiliated with American Express, asking him to follow a link to log-in to his “Serve”
15 account. Plaintiff Essar knew the email to be false because he did not have a “Serve” account
16 through American Express. Subsequently, in October 2016, Mr. Essar received an email
17 notice from Yahoo notifying him of the 2014 Breach, and informing him that his Yahoo
18 accounts and PII may have been compromised. As a result of the breach notification, and
19 concerned for his own and his family’s well-being, Plaintiff Essar signed up for a credit
20 counseling class through his employer to learn how to limit, recognize, and respond to
21 identity theft. In addition, as a direct result of the 2014 Breach, Mr. Essar signed up for and
22 paid (and continues to pay) \$35.98 per month for LifeLock credit monitoring service.
23 Notwithstanding his attempts to limit the damage done to his credit and identity as a result of
24 the 2014 Breach, Mr. Essar has suffered great harm as a result of the Breach. Plaintiff Essar
25 not only lost years of email messages when several hundred simply vanished from his Yahoo
26 account, he also experienced tax fraud in February 2017, when an unauthorized person
27 fraudulently filed a tax return under his Social Security Number. Further, Mr. Essar was
28 denied credit in March 2017 due to the identity theft he suffered as a result of the 2014

1 Breach, and freezes were placed on his credit. Because Plaintiff Essar is a United States
2 citizen of Afghani descent, he worries that a terrorist sympathizer may steal his PII and may
3 use it to commit crimes in his name, so much so that he suffers from extreme anxiety and has
4 difficulty sleeping. Finally, the Yahoo Data Breaches have caused Plaintiff Essar to be at
5 substantial risk for further identity theft.

6 20. Plaintiff Paul Dugas is a resident and citizen of San Diego, California.
7 Plaintiff Dugas is a semi-retired real estate investor and banker. Mr. Dugas has opened four
8 Yahoo accounts over approximately the last twenty years. He used his Yahoo accounts for
9 his banking, investment accounts, business emails, and personal emails. Plaintiff Dugas's
10 2013 and 2014 business tax returns were compromised, and he is still attempting to resolve
11 the matter. As a result, his business has had to pay penalties and otherwise has been
12 financially penalized. In April 2016, Plaintiff Dugas was unable to file his personal tax return
13 because the Internal Revenue Service stated that a tax return had already been filed under his
14 Social Security Number. As a result of his inability to file a tax return in 2016, both of his
15 college-aged daughters missed deadlines to submit the Free Application for Federal Student
16 Aid (FAFSA). Because Plaintiff Dugas' daughters were unable to file for FAFSA, he paid
17 \$5,000 tuition for one daughter and \$4,000 room and board for the other—expenses that he
18 would not have had to cover had his daughters been able to file for FAFSA, as they had in
19 the past. Plaintiff Dugas also experienced numerous fraudulent charges on his personal and
20 business Bank of America and Navy Federal Credit Union credit cards. He has had to replace
21 his Bank of America credit card numerous times and his Navy Federal credit card once.
22 Plaintiff Dugas has paid \$30.00 to three different credit bureaus to freeze his accounts. In
23 addition, Plaintiff Dugas paid extra fees and costs to his Certified Public Accountant to help
24 sort out the tax return problems suffered as a result of the Breach. Finally, the Yahoo Data
25 Breaches have caused Plaintiff Dugas to be at substantial risk for further identity theft.

26 21. Plaintiffs Matthew and Deana Ridolfo are a married couple and residents and
27 citizens of Vineland, New Jersey. Plaintiff Deanna Ridolfo works with a public school
28 system and Plaintiff Matthew Ridolfo is a mechanical designer for a local company. Both

1 Plaintiffs used their Yahoo accounts for nearly twenty years for general banking, credit card
2 management and communications, a mortgage refinance, and communication with friends
3 and family. In June 2016, Plaintiff Matthew Ridolfo used his Yahoo email account to send
4 scanned copies of sensitive financial documents in order to refinance the couple's home
5 mortgage. Shortly thereafter, in December 2016, both Mr. and Mrs. Ridolfo received notice
6 of the 2013 Breach. On January 4, 2017, Plaintiff Deana Ridolfo received a letter from
7 Citibank informing her that Citibank was concerned that her Citibank card was fraudulently
8 accessed. Since Plaintiff Deana Ridolfo had never opened a Citibank account, she
9 immediately knew it was a fraudulent card. Mrs. Ridolfo contacted Citibank immediately and
10 learned that cash advances and Uber charges were listed on the account that had been opened
11 in her name. Citibank also informed her that a second Citibank account was recently applied
12 for in her name, this one for a Sears branded credit card. As a result of the letter and
13 information received from Citibank, the Ridolfos immediately obtained free credit reports
14 through Experian. Plaintiff Deana Ridolfo learned that someone attempted to open an
15 account at Barclay Bank, two accounts at Lowes, and a Walmart account in her name.
16 Further, Mrs. Ridolfo learned that an American Express account was fraudulently opened in
17 her name, and \$900.00 had been charged on a fraudulently opened Target credit card. Mr.
18 Ridolfo learned that a total of eleven credit card or bank accounts had been fraudulently
19 opened or attempted to be opened during the month of December 2016 in his name through
20 the following retailers and banks: Brooks Brothers, Brandsource, Citi Doublecash, Capital
21 One, Walmart, Lowes, Sears Mastercard, TD Bank, Barclays Bank of Delaware, Santander
22 Bank, and Banco Popular of Puerto Rico. In addition, fraudulent addresses were listed for the
23 Ridolfos in Florida and Virginia. As a result of this significant fraud, both Plaintiffs Matthew
24 and Deana Ridolfo were forced to individually call each bank to report the fraudulent
25 accounts and charges, spending significant time talking with credit card fraud departments.

26 22. Further, unauthorized persons hacked into the Ridolfos' personal home phone
27 line through Comcast and forwarded their home line phone calls to an unknown phone
28 number. Plaintiffs Matthew and Deana Ridolfo made countless phone calls to credit card

1 companies, Experian, TransUnion, Equifax, Innovis, the Internal Revenue Department, the
2 Department of Motor Vehicles, and the Social Security Administration to help protect their
3 sensitive and confidential information. Further, the Ridolfos were forced to file police reports
4 in New Jersey, Florida and Virginia to protect their identity. In addition, Plaintiffs Matthew
5 and Deana Ridolfo purchased and enrolled in LifeLock to have help monitoring their credit
6 and finances, expending approximately \$30.00 per month each for a total of over \$60.00 per
7 month. Despite enrolling in a credit monitoring program, placing freezes on their credit, and
8 individually notifying credit card companies and banks, an unauthorized person attempted to
9 open another credit card account on January 31, 2017 in Plaintiff Deana Ridolfo's name. On
10 June 26, 2017, Deana and Matthew Ridolfo were contacted by the Miami-Dade State
11 Attorney's Office regarding the arrest of a parolee whom police later found to be in
12 possession of a "journal" containing a list of approximately 200 names with additional
13 personal identifying information next to each name. Among those listed, according to the
14 State Attorney's Office, were Matthew and Deana Ridolfo. Next to Matthew's name was his
15 Yahoo email address and Yahoo account password (used up until Yahoo prompted a
16 password change following the breach announcements) as well as the Sears credit card
17 number fraudulently opened in Mr. Ridolfo's name. Next to Deana's name was the Citibank
18 credit card number also fraudulently opened in her name. Finally, the Yahoo Data Breaches
19 have caused Plaintiffs Matthew and Deana Ridolfo to be at substantial risk for further
20 identity theft.

21 **B. Class Representatives for the Israel Class**

22 23. Plaintiff Yaniv Rivlin is a resident of Tel Aviv, Israel, and has dual Israeli and
23 Canadian citizenship. Plaintiff Rivlin opened his Yahoo email account in Israel
24 approximately ten years ago mainly for personal purposes, including banking, friends and
25 family, credit card statements, and social security administration. Plaintiff Rivlin pays Yahoo
26 annually \$20.00 to have Yahoo emails received forwarded to another email account. Plaintiff
27 Rivlin maintains a credit card on file with Yahoo to pay for the forwarding service. Plaintiff
28 Rivlin was notified by Yahoo on December 20, 2016 that his Yahoo email account had been

1 breached. After the notification, Plaintiff Rivlin noticed an increase in unsolicited emails,
2 including spam and advertisements. Plaintiff Rivlin also spent, and continues to spend, time
3 and effort proactively changing username and passwords on many of his accounts to prevent
4 fraud. In addition, the Yahoo Data Breaches have caused Plaintiff Rivlin to be at substantial
5 risk for identity theft, if in fact his identity has not already been stolen.

6 24. Plaintiff Mali Granot is a resident and citizen of Raanana, Israel. Plaintiff
7 Granot maintained a Yahoo email account, which she opened in Israel in the fall of 1998, for
8 personal reasons, specifically to correspond with family, friends, and school. Plaintiff Granot
9 was unexpectedly locked out of her Yahoo email account and unable to gain access. Plaintiff
10 Granot eventually gained access to her Yahoo email account by answering security
11 questions. However, once she opened her Yahoo email account, she received unsolicited
12 pop-up chat requests and other unsolicited requests including for services that she had not
13 requested but that someone had requested in her name using her Yahoo email account. In
14 addition, the Yahoo Data Breaches have caused Plaintiff Granot to be at substantial risk for
15 identity theft, if in fact her identity has not already been stolen.

16 **C. Class Representative for the Small Business Users Class**

17 25. Plaintiff Brian Neff is a citizen and resident of Texas. In September 2009, in
18 connection with his online insurance agency business, he contracted with Yahoo for two
19 services, Yahoo! Web Hosting for www.TheInsuranceSuite.com and Yahoo! Business Email,
20 for which he paid Yahoo \$13.94 every month from September 2009 through approximately
21 June 2017. Before contracting with Yahoo for these services, Mr. Neff read the applicable
22 Terms of Service and the website content regarding those services thoroughly and carefully
23 and relied upon, among other provisions, Yahoo's contractual commitments and
24 representations that his PII would be secure. Between 2009 and the present, at various times,
25 Plaintiff Neff used Defendants' web hosting services in connection with another 54 websites,
26 paying anywhere from \$3.94 to \$15.94 per month for each website. Prior to contracting with
27 Yahoo or Aabaco for each of these websites, Mr. Neff reviewed the Terms of Service and
28 website content for major changes, and each time he relied upon Yahoo's or Aabaco's

1 contractual commitments and representations that his PII would be secure. In addition, every
2 time Yahoo or Aabaco made changes to the Terms of Service and notified him of same, Mr.
3 Neff carefully reviewed the changes, and each time he relied upon Yahoo's or Aabaco's
4 contractual commitments and representations that his PII would be secure.

5 26. On December 14, 2016, Plaintiff Neff received a notice from Yahoo
6 informing him that hackers had stolen account information that he had provided to
7 Defendants—information that “may have included names, email addresses, telephone
8 numbers, dates of birth, hashed passwords [using outdated encryption] and, in some cases,
9 encrypted or unencrypted security questions and answers.” In addition to losing the benefit of
10 his bargain by paying, and overpaying, Yahoo thousands of dollars for services that subjected
11 him to security breaches (damaging him in the full amount of those payments), Plaintiff Neff
12 was also a victim of actual identity theft, which, upon information and belief, was caused by
13 one or more of the Yahoo Data Breaches. In May 2015, Plaintiff Neff incurred fraudulent
14 charges on his Capital One credit card and his Chase debit card, both of which were on file
15 with Yahoo to pay for services connected with two of his websites, with Yahoo being the
16 only company to which Plaintiff Neff had provided information about both accounts. In
17 addition to these fraudulent charges, also in May 2015, an unauthorized credit card account
18 in Plaintiff Neff's name was opened at Credit One Bank, and unauthorized and fraudulent
19 charges were made to that account in May and June 2015. Plaintiff Neff had to spend
20 significant time and incurred expenses mitigating the harm to him from these security
21 breaches and identity theft. As to both the Capital One and Chase cards, Plaintiff Neff had to
22 make several phone calls to each to notify them of the fraudulent charges and to have the
23 accounts frozen. Plaintiff Neff had to change passwords for both cards and he then had to
24 wait two to four days to receive new cards from each. As to the Credit One Bank credit card
25 opened in his name, Plaintiff Neff had to call the police department and file a police report,
26 fill out an FTC affidavit, engage in multiple phone calls to Credit One over several weeks
27 totaling multiple hours, and put together a package of materials for Credit One, which took
28 hours, and which he sent to Credit One via Federal Express overnight delivery at a cost of

1 \$11.87. In addition, at a time when Plaintiff Neff was trying to pre-qualify for a home
2 mortgage, he learned that his credit reports contained negative information about over-limits
3 and unpaid charges on the fraudulent Credit One Bank credit card. He had to write a demand
4 letter to Credit One Bank to force it to contact Experian and TransUnion and have these
5 negative items removed from his credit reports. Mr. Neff has never been notified that he was
6 a victim of any other data breach.

7 27. Since these incidents, Plaintiff Neff has been reviewing reports from
8 complimentary credit monitoring offered by all his credit cards which offer that
9 complimentary service, reviewing daily updates from Credit Karma, and he has ordered and
10 reviewed free annual reports from all three credit bureaus—all activities to which he has been
11 required to devote many hours of time. Since he became aware of the inadequacy of
12 Defendants' online security, Plaintiff Neff stopped using the TheInsuranceSuite.com website,
13 costing him many valuable leads, in the range of 2,500–3,000, for his insurance business.
14 Further, Plaintiff Neff is in the process of migrating that website to a more secure provider.
15 The cost to transfer Plaintiff Neff's accounts and services currently with Defendants to a
16 company with adequate security will be in excess of \$10,000, due to the nature and capacity
17 of his website and the cost to reestablish the high search engine placement he had earned
18 over the last eight years, among other factors. Finally, the Yahoo Data Breaches have caused
19 Plaintiff Neff to be at substantial risk for further identity theft.

20 **D. Class Representative for the Paid Users Class**

21 28. Plaintiff Andrew J. Mortensen is a resident and citizen of Dallas,
22 Texas. Plaintiff Mortensen was a New Jersey, Oklahoma, and then Texas resident during the
23 pendency of the 2013, 2014 and Forged Cookie Data Breaches. Plaintiff Mortensen has been
24 a Texas resident since May 2014. Plaintiff Mortensen opened a Yahoo email account in or
25 around 2004, has paid Yahoo for services since 2007, and has used his email account for both
26 personal and business purposes. Plaintiff Mortensen has paid \$19.95 per year for Yahoo's
27 premium email service since December 2007. Plaintiff Mortensen received banking, credit
28 card, investment account, business emails, personal emails, bill pay information, medical,

1 and automobile information in his Yahoo account. Plaintiff Mortensen regularly used his
2 Yahoo email account to monitor and/or manage banking information, financial information,
3 and online bill payments, as well as to communicate and share personal information with
4 family and friends. Plaintiff Mortensen has experienced increased suspicious phone calls or
5 emails, including spam calls once a week, and spam texts every two weeks. As a result of
6 the Data Breaches, Plaintiff Mortensen was forced to expend approximately three hours of
7 time and effort checking credit and opening accounts (and will be forced to expend additional
8 time in the future), and has experienced anxiety as a result of the Data Breaches. Yahoo's
9 failure to timely and adequately notify its accountholders of the 2014 Data Breach put
10 Plaintiff Mortensen at greater risk of identity theft and other fraud. In or about December
11 2016, Plaintiff Mortensen received notice from defendant Yahoo that his PII had been
12 compromised due to a data breach. Plaintiff Mortensen was not notified by Yahoo without
13 unreasonable delay, and was injured as a result.

14 **E. Defendants**

15 29. Yahoo is a Delaware corporation registered with the California Secretary of
16 State, with its principal place of business and headquarters in Sunnyvale, California, located
17 at 701 First Ave., Sunnyvale, CA 94089. In June, 2017, Yahoo, Inc. completed the sale of
18 substantially all of its assets to Verizon. Yahoo continues to exist as a wholly-owned
19 subsidiary of Oath, Inc., a subsidiary of Verizon. The remaining assets of Yahoo, Inc. were
20 renamed Altaba.⁶

21 30. Aabaco is a wholly owned and controlled subsidiary of Yahoo. Its
22 headquarters and principal place of business are the same as Yahoo's headquarters in
23 Sunnyvale, California. Since November 2015, Aabaco has been the business entity that
24 Yahoo uses to provide services to small business owners. Before that date, Yahoo provided
25 the same services through one of its divisions, Yahoo Small Business. After the transition to
26 Aabaco, Yahoo reassured its subscribers that the change was in name only, greeting them
27

28 ⁶ See fn. 1.

1 with the following account sign-in notice: “Yahoo Small Business is now Aabaco Small
2 Business. Same Team. Same Passion to grow your business. Different name.”

3 31. At all relevant times, Aabaco has been the alter ego of Yahoo for its small
4 business subscribers and has been wholly owned and managed by Yahoo. Yahoo and Aabaco
5 are also joint venturers and are jointly responsible to small business customers for any
6 wrongful acts carried out by Aabaco that are material to this suit. Finally, Aabaco is the
7 successor in interest to the Yahoo Small Business division and is liable to small business
8 customers, in addition to Yahoo, as the successor for any wrongdoing by that division before
9 it was renamed Aabaco.

10 **FACTUAL BACKGROUND**

11 **A. Yahoo Collects and Stores PII for its Own Financial Gain**

12 32. One of the web’s earliest pioneers, Yahoo was founded in 1994 as a directory
13 of websites, but quickly developed into a source for searches, email, shopping, and news.
14 Currently, its services attract at least one billion visitors per month. Yahoo sister sites include
15 Flickr, Yahoo Finance, and Yahoo Fantasy Sports, among others.

16 33. Yahoo’s primary service is Yahoo Mail, one of the oldest email services.
17 Many users have built their digital identities around Yahoo Mail, using the service for
18 everything from their bank and stock trading accounts to photo albums and even medical
19 information. Moreover, users not only use their Yahoo Mail accounts for private email
20 communications, but they also use them as recovery and log-in credentialing points for
21 accounts on many other websites. Yahoo allows anyone who is over the age of 12 to open a
22 Yahoo account.

23 34. Yahoo also offers various online services to small businesses. Popular
24 services include website hosting, which makes it easy for businesses to create and operate a
25 business website, advertising for those businesses, and email services for communications
26 between businesses and their customers. To obtain these services, small businesses or their
27 owners have to set up accounts with Yahoo and/or Aabaco and provide credit card or debit
28 card information for automatic monthly payments. Yahoo originally provided these services

1 through a division called Yahoo Small Business. Since November 2015, Yahoo has provided
2 its small business services through its wholly owned subsidiary Aabaco.

3 35. When users establish any of the above accounts with Defendants, users must
4 provide Defendants with PII, which Defendants then electronically collect, store on, and
5 route through its U.S.-based servers, a majority of which are located in California. And, in
6 fact, Plaintiffs and Class members signed up for online Yahoo accounts and provided the
7 required PII, including, in some cases, debit and credit card information, which, Defendants
8 collected, stored, and routed through its U.S.-based servers.

9 36. Plaintiffs and Class members signed up for online Yahoo accounts that
10 required them to provide many different sorts of personal information, including, in some
11 cases, debit and credit card information.

12 37. The “Privacy Center” portion of Yahoo’s website delineates the type of
13 personal information it collects directly from its account holders.⁷ Yahoo’s Privacy Policy,
14 which is incorporated by reference into the Terms of Service to which all users must agree
15 when they create their accounts, explains⁸:

Information Collection & Use

General

Yahoo collects personal information when you register with Yahoo, when you use Yahoo products or services, when you visit Yahoo pages or the pages of certain Yahoo partners, and when you enter promotions or sweepstakes. Yahoo may combine information about you that we have with information we obtain from business partners or other companies.

When you register we ask for information such as your name, email address, birth date, gender, ZIP code, occupation, industry, and personal interests. For some financial products and services we might also ask for your address, Social Security number, and information about your assets. When you register with Yahoo and sign in to our services, you are not anonymous to us.

Yahoo collects information about your transactions with us and with some of our business partners, including information about your use of financial products and services that we offer.

⁷ Yahoo Privacy Center, Yahoo!, <https://policies.yahoo.com/us/en/yahoo/privacy/index.htm> (last visited Apr. 5, 2017).

⁸ Yahoo’s Terms of Service for the years 2011-2016 are attached to this First Amended Consolidated Class Action Complaint as Exhibits 1 through 6, respectively. Yahoo’s Privacy Policies for those same years are attached as Exhibits 7-12, respectively.

1 38. Yahoo also informs its account holders that it shares personal information
2 provided by account registrants only under limited circumstances.⁹

Information Sharing & Disclosure

Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you've requested, when we have your permission, or under the following circumstances:

- We provide the information to trusted partners who work on behalf of or with Yahoo under confidentiality agreements. These companies may use your personal information to help Yahoo communicate with you about offers from Yahoo and our marketing partners. However, these companies do not have any independent right to share this information.
- We have a parent's permission to share the information if the user is a child under age 13. See [Children's Privacy & Family Accounts](#) for more information about our privacy practices for children under 13.
- We respond to subpoenas, court orders, or legal process (such as [law enforcement requests](#)), or to establish or exercise our legal rights or defend against legal claims.
- We believe it is necessary to share information in order to investigate, prevent, or take action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Yahoo's terms of use, or as otherwise required by law.
- We transfer information about you if Yahoo is acquired by or merged with another company. In this event, Yahoo will notify you before information about you is transferred and becomes subject to a different privacy policy.

Yahoo displays targeted advertisements based on personal information. Advertisers (including ad serving companies) may assume that people who interact with, view, or click targeted ads meet the targeting criteria—for example, women

15 39. Each time Yahoo made changes to its Terms of Service, Plaintiffs and the
16 members of the Class were required to accept the new Terms by way of a clickwrap
17 agreement. Plaintiffs who did not accept the new Terms of Service would not be able to
18 continue to use their Yahoo accounts.

19 40. At all times relevant herein, Yahoo represented and warranted to Plaintiffs and
20 the Class members that its databases containing PII were secure and that customers' PII
21 would remain private.

22 41. Yahoo made promises to Class members in its Privacy Policies, including¹⁰:

We limit access to personal information about you to employees who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs.

We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.

⁹ *Id.*

¹⁰ *See, e.g.*, Exh. 9, Yahoo! Privacy Policy – 2013.

1 42. In 2016, Yahoo updated its Privacy Policy to clarify the protections it
2 provided in connection with data transfer¹¹:

3 **Data Transfer**

4 Your personal information may be transferred to countries other than your own to process and store data in
5 accordance with our Privacy Policy and to provide you with products and services. Some of these countries may not
6 have the same data protection safeguards as the country where you reside. By using our products and services, you
consent to us transferring your data to these countries. We are committed to ensuring your information is protected
and apply safeguards in accordance with applicable law.

7 43. Yahoo made further guarantees on its “Security at Yahoo” page (hyperlinked
8 from Yahoo’s Privacy Policy)¹²:

9 **Security at Yahoo**

10 Protecting our systems and our users' information is paramount to ensuring Yahoo users enjoy a secure user experience and
11 maintaining our users' trust. We have taken the following measures to protect your information:

12 Secure Storage

13 We deploy industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect
14 your personal information.

15 44. None of these representations were true.

16 **B. Yahoo’s Small Business Customers Depended on Defendants’ PII Security Practices**

17 45. Defendants Yahoo and Aabaco understand that online security is paramount to
18 their Small Business customers and was and is highly material to their decision to use
19 Defendants’ Small Business services. Defendants address these concerns in the advertising
20 that Defendants present to all would-be customers exploring the Small Business services. All
21 customers, including Plaintiff Neff, were exposed to and read these advertisements and
22 explanations, which appear on the webpages all customers must use to sign-up for the
23 services.

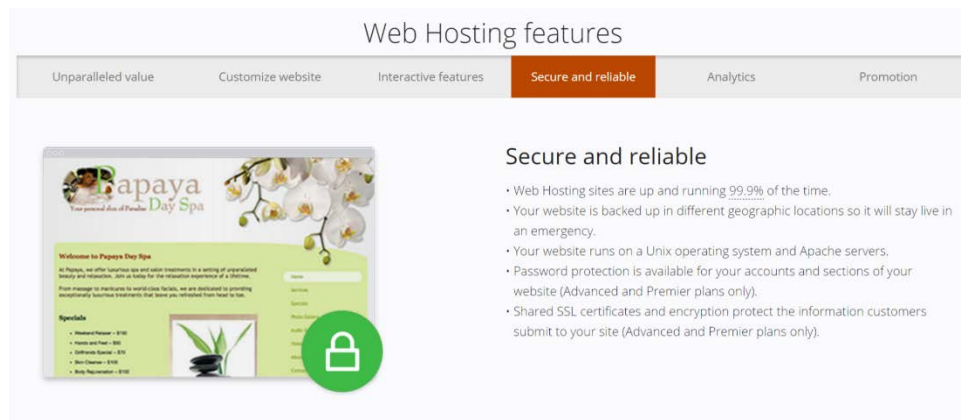
24 46. Defendants made similar representations about the importance of security on
25 Aabaco’s website as they did for Yahoo’s main page: “We have physical, electronic, and

26 ¹¹ Exh. 12, Yahoo! Privacy Policy – 2016.

27 ¹² Security at Yahoo, Yahoo!,
28 <https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm> (Attached as Exhibit 13). The current version of the “Security at Yahoo” page is attached as Exhibit 14.

procedural safeguards that comply with federal regulations to protect your Personal Information.”¹³ This page is attached to this First Amended Consolidated Class Action Complaint as Exhibit 15.

47. For example, the current web hosting advertisement and explanations page assures that web hosting is safe and secure¹⁴:



48. The relationship between Defendants and Small Business Class Members is governed by Defendants’ Terms of Service, which incorporate by reference a number of other agreements including Defendants’ Privacy Policy (“Privacy Policy”). Throughout the relevant time, the Terms of Service was a “click-through” agreement. Each member of the Small Business Users Class, including Plaintiff Neff, prior to becoming a Small Business customer, was required to click a box stating that “I agree to the terms of service,” with terms of service being a live link page that would open when clicked.¹⁵

¹³ Privacy Policy, Yahoo! Aabaco Small Business,

<https://www.aabacosmallbusiness.com/privacy-policy> (last visited Apr 9, 2017).

¹⁴ Flexible hosting for your professional website, Yahoo! Aabaco Small Business,

<https://smallbusiness.yahoo.com/webhosting#reliable> (last visited Apr. 12, 2017).

¹⁵ Account Creation and Login Page, Yahoo! Aabaco Small Business,

<https://login.luminate.com/>

registration?.src=smbiz&.done=https%3A%2F%2Fwww.luminate.com (last visited Apr. 5, 2017).

1 49. The Terms of Service expressly refer to both Aabaco and Yahoo¹⁶:

2 Terms of Service

3 < Terms of Service Center

4 This website and the services and products offered are provided by Aabaco Small
5 Business, LLC and its subsidiaries (the "Company") subject to the following Terms of
6 Service ("Terms"), which may be updated from time to time without notice to the user
7 ("You", "Your", or "Merchant"). The Company is a wholly-owned subsidiary of Yahoo! Inc
8 ("Yahoo"). By accessing and using this website and the services and products offered on it,
9 You accept and agree to be bound by the Terms. In addition, when using this website, the
 services, or products, You will be subject to any posted guidelines or rules applicable to
 such services, which may be posted and modified from time to time. All such guidelines
 and rules, including the [Privacy Policy](#), the [Site Guidelines](#), and certain third party
 agreements as described below, are hereby incorporated by reference into these Terms
 (all together, the "Agreement").

10 50. The Privacy Policy has been updated over the years but, as relevant to this
11 action, has always contained identical or substantively similar assurances that Defendants
12 appropriately safeguard the PII entrusted to them.¹⁷ The Privacy Policy in effect throughout
13 the relevant time represents that:

14 CONFIDENTIALITY AND SECURITY

15 We limit access to Personal Information about You to employees, contractors, or service
16 providers who we believe reasonably need to come into contact with that information to
 provide products or services to You or in order to do their jobs.

17 We have physical, electronic, and procedural safeguards that comply with federal
18 regulations to protect Personal Information about You.

19
20
21
22
23
24
25 ¹⁶ [Terms of Service](#), Yahoo! Aabaco Small Business, <https://smallbusiness.yahoo.com/tos>
26 (last visited Apr. 5, 2017).

27 ¹⁷ [Privacy Policy](#), Yahoo! Aabaco Small Business,
28 <https://www.aabacosmallbusiness.com/privacy-policy?updated=true> (last visited Apr. 5,
 2017).

1 51. In addition, the Privacy Policy represents that Defendants do not share PII
2 except in the following delineated circumstances¹⁸:

3 **INFORMATION SHARING AND DISCLOSURE**

4 The Company does not rent, sell, or share Personal Information about You with other
5 people or non-affiliated companies except to provide products or services You've
6 requested, when we have Your permission, or under the following circumstances:

- 7 • **Service Providers, Contractors, and Agents:** We provide information to partners
8 who work on behalf of or with the Company under confidentiality agreements.
9 These companies do not have any independent right to share this information.
- 10 • **Co-Branded Partners:** The Company may provide some services in partnership
11 with others under a co-branded experience. In these situations both companies
12 may be collecting information about You so please see the privacy links available
13 within the experience to learn more. For example, Business Mail is provided in
14 partnership with Yahoo.
- 15 • **Legal Process:** We respond to subpoenas, court orders, or legal process, or to
16 establish or exercise our legal rights or defend against legal claims.
- 17 • **Security & Fraud:** We believe it is necessary to share information in order to
18 investigate, prevent, or take action regarding illegal activities, suspected fraud,
19 situations involving potential threats to the physical safety of any person, violations
20 of the Terms of Service, or as otherwise required by law.
- 21 • **Merger & Acquisition:** We transfer information about You if the Company is
22 acquired by or merged with another company.

23 52. As Plaintiff Neff and the members of the Small Business Users Class would
24 discover in 2016, these material representations about security were false and misleading
25 because Defendants failed to disclose that their Small Business services were not secure, and
26 that the PII they would be entrusting to Defendants was not reasonably safeguarded.

27 53. Defendants collect and store tremendous amounts of PII, and use this
28 information to maximize profits through targeted advertising and other means. Defendants
also assure that they take user privacy and safeguarding of PII very seriously. The facts show
otherwise.

23 **C. PII is Very Valuable on the Black Market**

24 54. The types of information compromised in the Yahoo Data Breaches are highly
25 valuable to identity thieves. In addition to credit and debit card information, names, email
26 addresses, recovery email accounts, telephone numbers, birthdates, passwords and security
27

28 ¹⁸ *Id.*

question answers can all be used to gain access to a variety of existing accounts and websites. Indeed, Plaintiffs and Class members have suffered a variety of consequences from the breaches, including forged credit applications, the opening of unauthorized credit card accounts, fake tax returns being filed under their names, fraudulent charges, email hacks, unauthorized access to payment accounts such as PayPal and Western Union, gift cards being generated from their accounts without their consent, and numerous other identity theft-related damages.

55. Identity thieves can also use the PII to harm Plaintiffs and Class members through embarrassment, blackmail, or harassment in person or online, or to commit other types of fraud including obtaining ID cards or driver's licenses, fraudulently obtaining tax returns and refunds, and obtaining government benefits. A Presidential Report on identity theft from 2008 states that:

In addition to the losses that result when identity thieves fraudulently open accounts or misuse existing accounts, . . . individual victims often suffer indirect financial costs, including the costs incurred in both civil litigation initiated by creditors and in overcoming the many obstacles they face in obtaining or retaining credit. Victims of non-financial identity theft, for example, health-related or criminal record fraud, face other types of harm and frustration.

In addition to out-of-pocket expenses that can reach thousands of dollars for the victims of new account identity theft, and the emotional toll identity theft can take, some victims have to spend what can be a considerable amount of time to repair the damage caused by the identity thieves. Victims of new account identity theft, for example, must correct fraudulent information in their credit reports and monitor their reports for future inaccuracies, close existing bank accounts and open new ones, and dispute charges with individual creditors.¹⁹

¹⁹ The President's Identity Theft Task Force, Combating Identity Theft: A Strategic Plan, Federal Trade Commission, 11 (April 2007), <http://www.ftc.gov/sites/default/files/documents/reports/combating-identity-theft-strategic-plan/strategicplan.pdf>.

1 56. To put it into context, as demonstrated in the chart below, the 2013 Norton
2 Report, based on one of the
3 largest consumer cybercrime
4 studies ever conducted,
5 estimated that the global price
6 tag of cybercrime was around
7 \$113 billion at that time, with
8 the average cost per victim being
9 \$298 dollars. That number will
10 no doubt increase exponentially
11 after the massive Yahoo Data
12 Breaches.



13 57. The problems associated with identity theft are exacerbated by the fact that
14 many identity thieves will wait years before attempting to use the PII they have obtained.
15 Indeed, in order to protect themselves, Class members will need to remain vigilant against
16 unauthorized data use for years and decades to come.

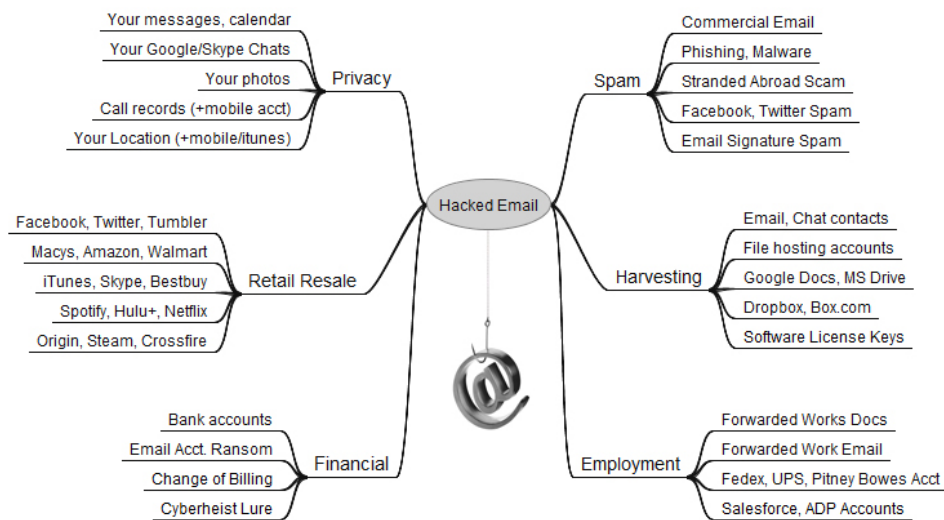
17 58. Once stolen, PII can be used in a number of different ways. One of the most
18 common is that it is offered for sale on the “dark web,” a heavily encrypted part of the
19 Internet that makes it difficult for authorities to detect the location or owners of a website.
20 The dark web is not indexed by normal search engines such as Google and is only accessible
21 using a Tor browser (or similar tool), which aims to conceal users’ identities and online
22 activity. The dark web is notorious for hosting marketplaces selling illegal items such as
23 weapons, drugs, and PII.²⁰ Websites appear and disappear quickly, making it a very dynamic
24 environment.

25
26
27 ²⁰ Brian Hamrick, The dark web: A trip into the underbelly of the internet, WLWT News
28 (Feb. 9, 2017 8:51 PM), <http://www.wlwt.com/article/the-dark-web-a-trip-into-the-underbelly-of-the-internet/8698419>.

59. Once someone buys PII, it is then used to gain access to different areas of the victim's digital life, including bank accounts, social media, and credit card details. During that process, other sensitive data may be harvested from the victim's accounts, as well as from those belonging to family, friends, and colleagues.

60. In addition to PII, a hacked email account can be very valuable to cyber criminals. Since most online accounts require an email address not only as a username, but also as a way to verify accounts and reset passwords, a hacked email account could open up a number of other accounts to an attacker.²¹

61. As shown below, a hacked email account can be used to link to many other sources of information for an identity thief, including any purchase or account information found in the hacked email account.²²



D. Yahoo Turns a Blind Eye to Gaping Holes in Its Security, Refusing to Upgrade After Repeated Intrusions and Negative Assessments

62. Yahoo has a storied, unfortunate history of inadequate and outdated data security. For at least the last decade and a half, Yahoo has been repeatedly put on notice that its security measures were not up to par, leaving users' PII at risk of theft. Rather than

²¹ Identity Theft and the Value of Your Personal Data, Trend Micro (Apr. 30, 2015), <https://www.trendmicro.com/vinfo/us/security/news/online-privacy/identity-theft-and-the-value-of-your-personal-data>.

²² Brian Krebs, The Value of a Hacked Email Account, KrebsOnSecurity (June 13, 2013, 3:14 PM), <https://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/>.

1 addressing the problems by upgrading its data security, Yahoo continued to use outdated
2 security methods long after vulnerabilities were brought to Yahoo's attention. Yahoo's
3 refusal to heed myriad warnings about its deficient data security, even after multiple
4 breaches, created the environment that permitted unauthorized users to abscond with
5 Plaintiffs and Class members' PII.

6 63. Yahoo's systems have been vulnerable to a wide variety of attack methods. In
7 2001, then-20-year-old hacker Adrian Lamo showed he could rewrite published articles on
8 Yahoo! News without even having to enter a password.²³

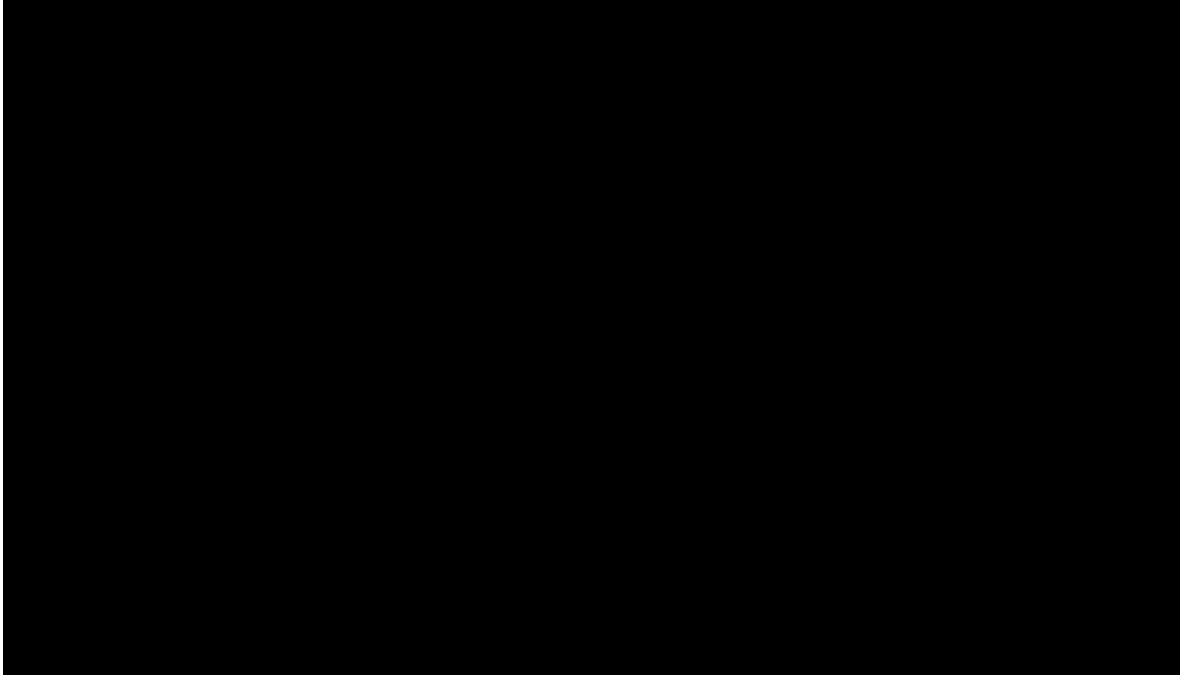
9 64. In 2008, multiple hosts on Yahoo's corporate network were compromised and
10 attackers targeted [REDACTED]
11 [REDACTED]

12 65. In 2009, the [REDACTED] attacks continued; [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]

17 66. In 2010 alone, Google informed Yahoo that Yahoo systems were being used
18 to attack Google, causing Yahoo to reopen a previously closed security investigation; Yahoo
19 discovered unauthorized access to its systems that predated the 2008 access identified above;
20 [REDACTED]
21 [REDACTED]

22
23
24
25
26
27
28 ²³ Kevin Poulsen, Yahoo! News Hacked, SecurityFocus (Sept. 18, 2001),
<http://www.securityfocus.com/news/254>.

1 67. In 2011, then- Chief Information Security Officer (CISO), a senior-level
2 executive at Yahoo, Justin Somaini presented at a third quarter Information Risk
3 Management All Hands meeting, identifying gaping holes in Yahoo’s data security:



15 68. [REDACTED]



17 69. With such major deficiencies, it was only a matter of time until a major
18 intrusion occurred. In late 2011, law enforcement notified Yahoo that its information
19 technology environment may have been breached.

20 70. More than a month later, on January 30, 2012, Yahoo retained Mandiant to
21 investigate and perform a Threat Assessment Program (TAP). Yahoo limited the assessment,
22 instructing Mandiant to “not perform Live Response or forensic analysis of any compromised
23 system.”

24 71. On February 9, 2012, Mandiant conducted a two-hour training session on
25 industry best practices for remediation activities. The following day, on the tenth, Yahoo
26 conducted a “remediation event.”

1 72. Less than a week later, on February 16, 2012, Yahoo was alerted by a third
2 party that a vulnerability existed within its systems that allowed people to [REDACTED]

3 [REDACTED]
4 73. Mandiant conducted its assessment between February 13 and April 3, 2012. In
5 its subsequent report, dated April 20, 2012, Mandiant identified the earliest evidence of a
6 related intruder on Yahoo’s networks as March 22, 2010, [REDACTED]

7 [REDACTED]
8 74. [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]

17 75. Mandiant detected at least two different attack groups in Yahoo’s systems,
18 with the most recent activity seen on April 1, 2012—[REDACTED]

19 [REDACTED]
20 [REDACTED]
21 [REDACTED]

22 76. [REDACTED]
23 [REDACTED]

24 77. Also in 2012, Yahoo admitted that more than 450,000 user accounts were
25 compromised through an SQL injection attack—with the passwords simply stored in plain
26 text. This breach revealed that Yahoo apparently had failed to take even basic precautions to
27 protect its customers’ data. Indeed, news outlets reported that “[s]ecurity experts were
28 befuddled ... as to why a company as large as Yahoo would fail to cryptographically store

1 the passwords in its database. Instead, they were left in plain text, which means a hacker
2 could easily read them.”²⁴

3 78. According to Marcus Carey, a security researcher at Rapid7, the 2012 hack
4 showed Yahoo was far behind the times. “It is definitely poor security. It’s not even security
5 101. It’s basic application development 101.”²⁵ Indeed, the Federal Trade Commission
6 considered SQL injection attacks a known—and preventable—threat as far back as 2003.²⁶

7 79. The 2012 hack was meant—and should have served—as a “wake up call” to
8 Yahoo that it had inadequate protections for users’ personal information. In fact, a message
9 purportedly left by the hackers on the webpage where the information was dumped claimed
10 as much:

11 We hope that the parties responsible for managing the security of this
12 subdomain will take this as a wake-up call, and not as a threat ... There
13 have been many security holes exploited in Web servers belonging to
14 Yahoo! Inc. that have caused far greater damage than our disclosure.
Please do not take them lightly.²⁷

15 80. Yahoo should have immediately invested in security upgrades following the
16 2012 hack, the Mandiant report, and all other previous vulnerabilities uncovered, but instead
17 it did the opposite.

18 81. Rather than increasing its security forces in 2013—now known to be the year
19 that information for *all* Yahoo accounts was exfiltrated—Yahoo’s security staff dropped
20 from 62 employees to 43, including the departure of its CISO, Justin Somaini. Somaini
21 reportedly left due to disagreements with CEO Marissa Mayer’s management style. Yahoo
22 left the position vacant for more than a year, until March 2014.

23 ²⁴ Antone Gonsalves, Yahoo security breach shocks experts, CSO (July 12, 2012, 8:00 AM),
24 [http://www.csoonline.com/article/2131970/identity-theft-prevention/yahoo-security-breach-](http://www.csoonline.com/article/2131970/identity-theft-prevention/yahoo-security-breach-shocks-experts.html)
25 [shocks-experts.html](http://www.csoonline.com/article/2131970/identity-theft-prevention/yahoo-security-breach-shocks-experts.html).

26 ²⁵ *Id.*

27 ²⁶ In the Matter of Guess?, Inc., and Guess.com, Inc., FTC Matter No. 022 3260, 3 (Jul. 30,
2003), available at
<https://www.ftc.gov/sites/default/files/documents/cases/2003/08/guesscomp.pdf>.

28 ²⁷ Doug Gross, Yahoo hacked, 450,000 passwords posted online, CNN (July 13, 2012, 9:31
AM), <http://www.cnn.com/2012/07/12/tech/web/yahoo-users-hacked/>.

1 82. What is more, Yahoo detected multiple security problems throughout 2013,
2 working with outside cybersecurity firms to investigate the issues. Each time, numerous
3 vulnerabilities were identified. Each time, Yahoo chose to stick its proverbial head in the
4 sand rather than fix the problems.

5 83. One recurrent problem Yahoo steadfastly refused to fix was the issue of
6 inadequate logging standards. This inadequacy comes up again and again in the security
7 reports prepared for Yahoo. Dell SecureWorks (“DSW”), which Yahoo engaged multiple
8 times from 2013 through 2016, raised the issue with Yahoo repeatedly. During one such
9 2013 incident, internal code name “Project Dickens,” data from up to 64 million user
10 accounts appeared to be impacted, with anywhere from 16-23 million involved in a spam
11 email campaign.

12 84. Based on the spike in spam emails, DSW was retained to investigate potential
13 account compromise in the Yahoo User Database (UDB) environment.

14 85. [REDACTED]
15 [REDACTED]
16 [REDACTED]

17 86. [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]
22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]
28 [REDACTED]

1 [REDACTED]
2 [REDACTED]
3 [REDACTED]
4 87. In other words, DSW flagged a very serious vulnerability, but it could not
5 fully evaluate it due to the lack of audit capability on a particular system.

6 88. Yahoo also retained Leaf SR to conduct a security assessment of Yahoo's
7 UDB environment around the same time in 2013. [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]

15 89. Unfortunately, Yahoo's culture actively discouraged emphasis on data
16 security. For example, former Yahoo security staffers interviewed later told Reuters that
17 requests made by Yahoo's security team for new tools and features such as strengthened
18 cryptography protections were, at times, rejected on the grounds that the requests would cost
19 too much money, were too complicated, or were simply too low a priority.²⁸

20 **E. Yahoo's Inadequate Data Security Allows the Massive Breach of 3 Billion User**
21 **Accounts in 2013, Which Yahoo Then Fails to Disclose**

22 90. As an example of Yahoo's refusal to keep abreast of cybersecurity issues, in
23 the summer of 2013, Yahoo decided to finally abandon the use of a discredited technology
24 for encrypting data known as MD5. MD5 was well known as a weak password protection
25 method by hackers and security experts for years before the 2013 Breach. MD5 can be
26

27 _____
28 ²⁸ Reuters, Why Yahoo's Security Problems Are a Story of Too Little, Too Late, FORTUNE
(Dec. 18, 2016), <http://fortune.com/2016/12/19/yahoo-hack-cyber-security/>.

1 cracked more easily than other so-called “hashing” algorithms, which are mathematical
2 functions that convert data into seemingly random character strings.²⁹

3 91. In fact, five years before Yahoo finally took action, Carnegie Mellon
4 University’s Software Engineering Institute issued a public warning to security professionals
5 through a U.S. government-funded vulnerability alert system, stating that: MD5 “should be
6 considered cryptographically broken and **unsuitable for further use**.”³⁰

7 92. “MD5 was considered dead long before 2013,” said David Kennedy, chief
8 executive of cyber firm TrustedSec. “Most companies were using more secure hashing
9 algorithms by then.”³¹ Common techniques such as “salting” (adding a unique secret to the
10 password) and “stretching” (repeating the hashing process over many times) hashed
11 passwords makes them far harder for hackers to decode.³² Stronger hashing technology
12 would have made it more difficult for the hackers to get into customer accounts after
13 breaching Yahoo’s network, making the attack far less damaging, according to five former
14 employees and outside security experts.³³ But with MD5, there are vast indexes of these pre-
15 computed MD5 hashes—known as “rainbow tables”—freely available online that can be
16 used to quickly crack a large percentage of any MD5 password list.³⁴ In other words, since
17 the formula for breaking MD5 encryption was known since 2010 or earlier, simple online
18 tools could break even “salted” MD5 codes.

19
20
21 ²⁹ Reuters, Why Yahoo’s Security Problems Are a Story of Too Little, Too Late, FORTUNE
(Dec. 18, 2016), <http://fortune.com/2016/12/19/yahoo-hack-cyber-security/>.

22 ³⁰ Vulnerability Note VU#836068, Vulnerability Notes Database (Last revised Jan. 21,
2009), <https://www.kb.cert.org/vuls/id/836068>.

23 ³¹ Reuters, *supra* note 22.

24 ³² Mark Stockley, Yahoo breach: I’ve closed my account because it used MD5 to hash my
password, naked security (Dec. 15, 2016),
25 [https://nakedsecurity.sophos.com/2016/12/15/yahoo-breach-ive-closed-my-account-because-](https://nakedsecurity.sophos.com/2016/12/15/yahoo-breach-ive-closed-my-account-because-it-uses-md5-to-hash-my-password/)
26 [it-uses-md5-to-hash-my-password/](https://nakedsecurity.sophos.com/2016/12/15/yahoo-breach-ive-closed-my-account-because-it-uses-md5-to-hash-my-password/); Adam Bard, 3 Wrong Ways to Store a Password,
adambard.com (July 11, 2013), [https://adambard.com/blog/3-wrong-ways-to-store-a-](https://adambard.com/blog/3-wrong-ways-to-store-a-password/)
27 [password/](https://adambard.com/blog/3-wrong-ways-to-store-a-password/).

28 ³³ Stockley, *supra* note 26; Bard, *supra* note 26.

³⁴ Brian Krebs, My Yahoo Account Was Hacked! Now What?, KrebsOnSecurity (Dec. 15,
2016), <https://krebsonsecurity.com/2016/12/my-yahoo-account-was-hacked-now-what/>.

1 93. So, when Yahoo finally got around to discontinuing MD5 in late summer of
2 2013, its encryption was already years out-of-date.

3 94. Yahoo's failure to move away from MD5 in a timely fashion was indicative of
4 systemic problems in Yahoo's security operations. One cybersecurity expert said, "even by
5 2013 anyone with half a clue in securing passwords already long ago knew that storing
6 passwords in MD5 format was no longer acceptable and altogether braindead idea. It's one of
7 many reasons I've encouraged my friends and family to ditch Yahoo email for years."³⁵

8 95. Indeed, Yahoo's own security personnel often relied on external instant and
9 group messaging programs, like ██████████³⁶ and ██████████,³⁷ to communicate with each other in
10 order to protect themselves so their communications would not show up on Yahoo's network.

11 96. As a logical consequence of a highly reckless approach to security, Yahoo's
12 systems suffered a catastrophic breach in 2013, when hackers breached all then-existing
13 Yahoo UDB accounts—approximately three billion—stealing the poorly encrypted
14 passwords and other information in the biggest known data breach, by number of records
15 breached, to date. To make matters worse, Yahoo has experienced other security breaches
16 since the 2013 Breach occurred but before either the 2013 Breach or 2014 Breach was made
17 public in 2016. For example, in late December 2013, hackers found an exploit targeting Java
18 in Yahoo's ad network, which affected primarily users in Europe and was infecting roughly
19 27,000 computers *per hour* at the time of discovery.³⁸

20 97. None of these intrusions or reports prompted Yahoo to comprehensively
21 review and ameliorate its security protocols, allowing the 2014 Breach and the Forged
22 Cookie Breach to occur soon thereafter.

23
24
25
26 ³⁵ *Id.*

27 ██████████

28 ³⁸ Andrew Scurria, European Yahoo Users Victimized in Malware Attack, Law360 (Jan. 6, 2014, 6:02 PM), <https://www.law360.com/articles/498914/>.

1 **F. Yahoo's Security Is Breached Again and Again—in 2014, 2015, and 2016—Yet**
2 **Yahoo Still Does Not Alert Its Users**

3 98. Yahoo worked with DSW again in 2014, [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]

8 99. These repeated intrusions and warnings from professionals Yahoo itself hired
9 should have driven immediate action. Yahoo took a different tack.

10 100. [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]

17 101. [REDACTED]
18 [REDACTED]
19 [REDACTED]
20 [REDACTED]
21 [REDACTED]

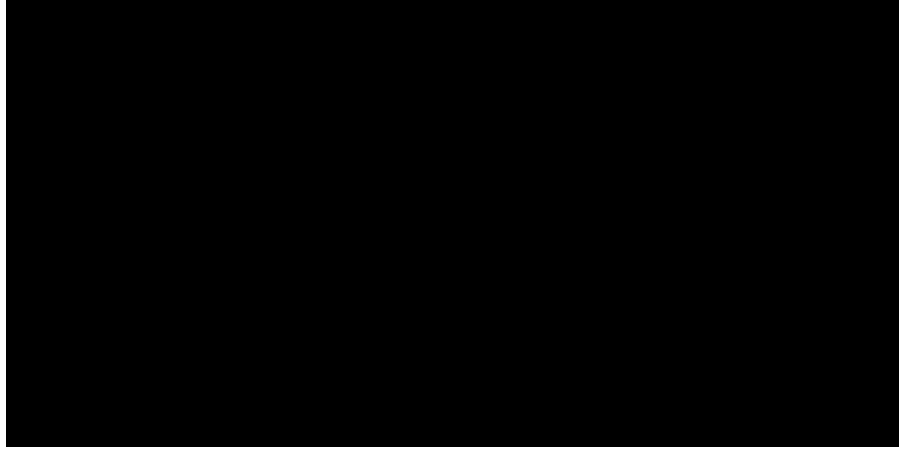
22 102. Then, in late 2014, hackers again accessed Yahoo UDB, accessing and taking
23 information from at least 500 million user accounts. Yahoo knew about the 2014 Breach
24 while it was happening, and even gave it an internal code name: "Siberia":

25	10.13.14, 11:39	Andrew R.	I need your help!
26	10.13.14, 12:18	Jeff Z.	whats up bud
27	10.13.14, 12:18	Andrew R.	I need a good investigation
28			name for this thing

[...]

1			
2	10.13.14, 12:19	Andrew R.	my first thought was
3			codename dingleberry
4	10.13.14, 12:20	Andrew R.	seems like no matter what
5			shit it's put through it's
6			just hanging on
7	10.13.14, 12:20	Jeff Z.	haha, clever but no go
8	10.13.14, 12:20	Andrew R.	hahah that should be more
9			like our team name
10	10.13.14, 12:20	Jeff Z.	that's fair
11	10.13.14, 12:21	Jeff Z.	lets go with a Russian
12			theme, either a city name or
13			famous figure
14	10.13.14, 12:21	Jeff Z.	since it's the Russians
15	10.13.14, 12:21	Andrew R.	true
16	10.13.14, 12:22	Andrew R.	stalin!
17	10.13.14, 12:23	Jeff Z.	I don't like Stalin
18	10.13.14, 12:23	Andrew R.	exactly!
19	10.13.14, 12:25	Andrew R.	just joking.. I'll give it
20			some thought
21	10.13.14, 12:27	Jeff Z.	I was thinking Project
22			Lenin, Project Runway, or
23			Project Siberia
24	10.13.14, 12:27	Jeff Z.	the second one is a joke
25	10.13.14, 12:32	Andrew R.	lol, siberia sounds pretty
26			cool
27	10.13.14, 12:33	Jeff Z.	lets do it
28			

1 103. Yahoo knew in 2014 that the Siberia intruder(s) had been in its systems for
2 months:

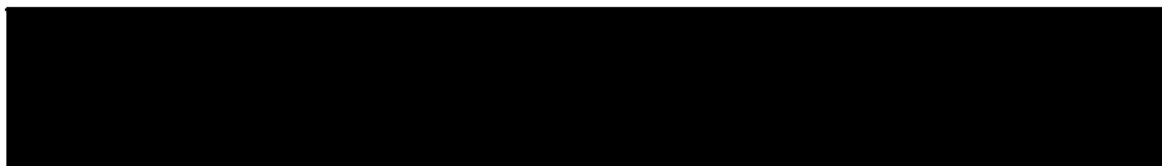
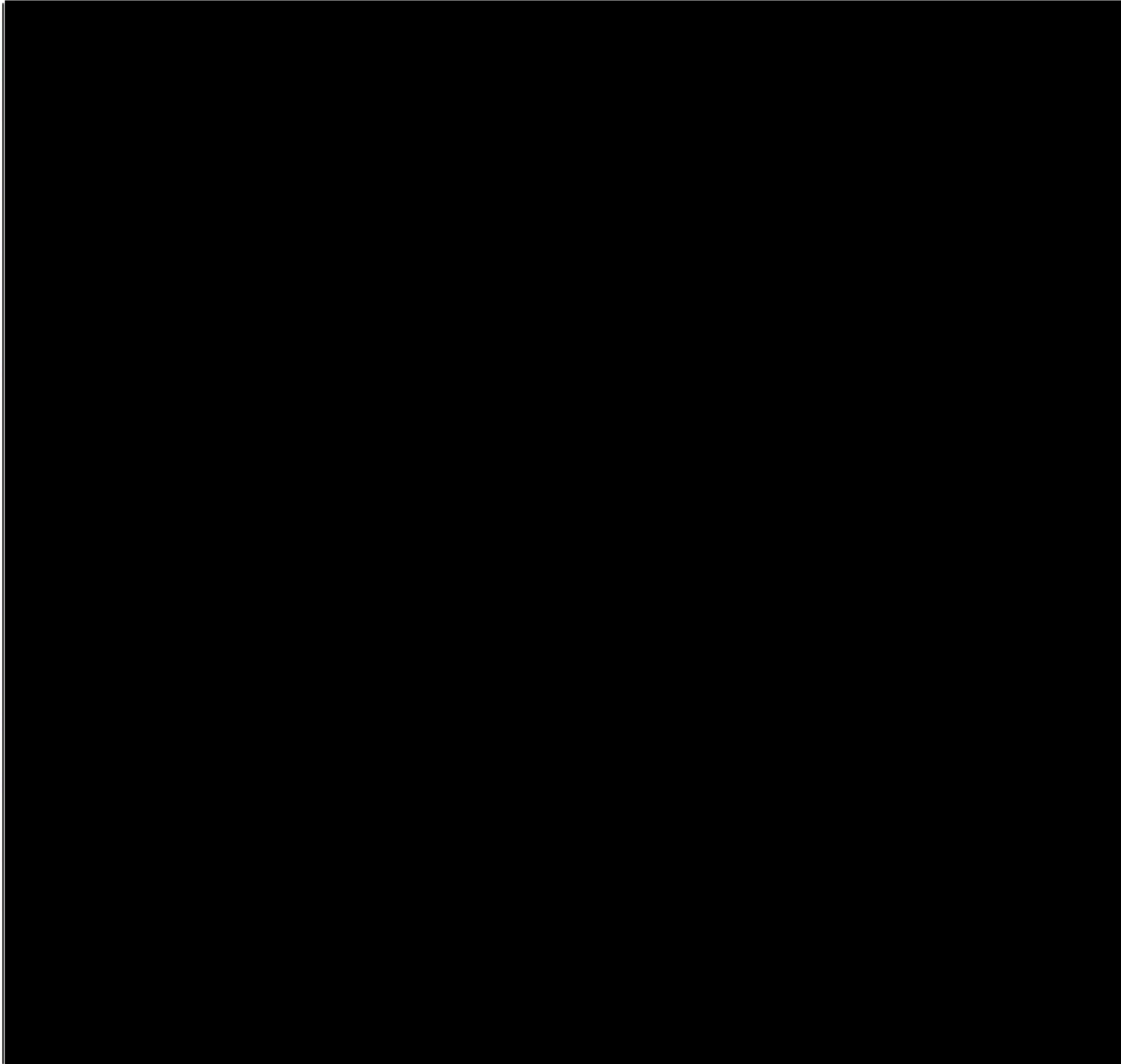


3
4
5
6
7
8
9 (From internal Yahoo PowerPoint revised Dec. 10, 2014)

10 104. Not only was Yahoo’s CISO aware of the 2014 Breach as it was happening,
11 Yahoo’s legal department was also contemporaneously aware of the 2014 Breach. Ron Bell,
12 then *General Counsel for Yahoo*, prepared a document indicating “600m accounts exposed”
13 and “100m transferred off.”

14 105. Yahoo also knew the attackers had actual access to multiple email accounts,
15 including CEO Marissa Mayer’s, via the AMT.
16
17
18
19
20
21
22
23
24
25
26
27
28

1 106. On December 8, 2014, Yahoo retained DSW yet again. The subsequent report,
2 issued February 10, 2015, showed several waves of attacks, distinguishing between the initial
3 “Siberia” intrusion and a later “Riviera” intrusion during early 2015:



24 While correctly showing that Yahoo had not, in fact, successfully expelled intruders in 2014,
25 this timeline was still not the full story. That would not come to light for several more years.

26 107. Adding insult to injury, Yahoo made no disclosures to its users about the
27 breach—no email warnings, no public notices, and no communications, other than emails to
28 “several dozen” individual users telling them to change their passwords and that their

1 account was “recently accessed by an unauthorized third party.” The vast majority of users
2 heard nothing for two full years while Yahoo sat on this information and sophisticated
3 identity thieves had free run of Class members’ PII and any confidential information that
4 could be acquired by using that PII. Defendants’ failure to take action and notify Class
5 members also prevented unknowing Class members from taking action, thus leaving them
6 even more vulnerable for a long period of time.

7 108. Yahoo did take *some* action in case news of the 2014 Breach got out—by
8 drafting a reactive press release. Rather than proactively notifying its users (potentially as
9 required by law) and demonstrating that it took security of user data seriously, Yahoo chose
10 to cross its fingers and hope no one found out.

11 109. [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]

19 110. Bob Lord became CISO at Yahoo in October 2015. He was deeply troubled
20 by what security and endemic culture issues faced him at Yahoo:

- 21 • “The decision to keep users at risk over engineering preference is an
22 example of the real culture of security.” – Bob Lord, CISO, 1.4.16
 - 23 • “we don’t have a **culture of security** in engineering, or at the executive
24 level” – Bob Lord, CISO, 2.5.16
- 25
26
27
28

111. Indeed, a brief online chat between Lord and Chris Rohlf neatly sums up the multilayered problems at Yahoo:

From: "lord@yahoo-inc.com" <lord@yahoo-inc.com>
To: <chrisrohlf@yahoo-inc.com>
Subject: <https://docs.google.com/document/d/1LUL2y7dpqnVMAYWKLuwS8SulOkB2JnYQlfiZB6rCviY/edit#heading=h.r03mluvyoo46>
Received: 26 Jan 2016 15:22:23 +0000 (UTC)

chrisrohlf@yahoo-inc.com(15:02:08 (UTC)):so traditionally ramses, alex, and ricky played siberia very close to the chest bec of the fear of it leaking to nytimes. It was never mine to make the call so I just went along
chrisrohlf@yahoo-inc.com(15:02:13 (UTC)):but i am def behind sharing more with paranoids at a minimum
lord@yahoo-inc.com(15:03:35 (UTC)):This could have been played two ways: (1) tell the org and work with people to improve our posture. (2) Don't tell the org, but have the CEO tell all L2s and L3s "Do what the CISO says. I know it's going to slow things down for a while. Can't say more."
lord@yahoo-inc.com(15:03:45 (UTC)):we did (3) Don't tell anyone, and don't empower the Paranoids
lord@yahoo-inc.com(15:04:07 (UTC)):oh, there's my WTF moment for the day!
chrisrohlf@yahoo-inc.com(15:04:24 (UTC)):yep. i know mm and some L3s knew bec they had to help do stuff like push Duo over a weekend
chrisrohlf@yahoo-inc.com(15:04:31 (UTC)):but yah, we swept it under the carpet
chrisrohlf@yahoo-inc.com(15:04:33 (UTC)):-\n lord@yahoo-inc.com(15:05:45 (UTC)):You can tell Jay's staff "This isn't a theoretical issue. We know for a fact that we're up against nation states, and it can get ugly." If that leaks to the NYTimes, it's a non issue
lord@yahoo-inc.com(15:06:25 (UTC)):I'm sure Son of Siberia is reading this and my mail, but at this point what can you do
chrisrohlf@yahoo-inc.com(15:06:34 (UTC)):agree. and honestly even it did the correct answer imo is "yes of course we have nation state attackers. what do you think we defend against everyday? why do you think we are here?"
chrisrohlf@yahoo-inc.com(15:06:45 (UTC)):hah we actually had an incident we called son of siberia
chrisrohlf@yahoo-inc.com(15:07:23 (UTC)):the technical details of which are so unbelievably lame you would cringe
lord@yahoo-inc.com(15:07:59 (UTC)):where is the final Siberia write up? I can't find a complete document.
lord@yahoo-inc.com(15:08:15 (UTC)):I can find tons of working docs, but not a postortem doc
chrisrohlf@yahoo-inc.com(15:08:30 (UTC)):it is a collection of documents created by rickys team. there may have been one single doc alex took to the board with ramses but if it exists i dont have access
lord@yahoo-inc.com(15:09:24 (UTC)):There was one board deck with a slide called "Nation State Update" in one, but it only had some speaker notes.
lord@yahoo-inc.com(15:09:30 (UTC)):Looks like nothing was shared in writing
chrisrohlf@yahoo-inc.com(15:10:33 (UTC)):the culture here has tended to treat incidents like individual machine compromises and not larger campaigns

112. To be clear, it appears from this exchange that Yahoo's senior executive in charge of information security at Yahoo assumed a nation state actor was contemporaneously reading his Yahoo emails, and Yahoo's employees admitted its approach to the Siberia intrusion was to sweep it under the rug.

113. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

114. [REDACTED]

1 115. Lord further discovered that many of the security vulnerabilities he was facing
2 at Yahoo in 2016 were unchanged from the problems Yahoo knew about in 2011³⁹:

3 [REDACTED]
4 [REDACTED]
5 [REDACTED]
6 [REDACTED]
7 [REDACTED]
8 [REDACTED]
9 [REDACTED]
10 [REDACTED]
11 [REDACTED]
12 [REDACTED]
13 [REDACTED]
14 [REDACTED]
15 [REDACTED]
16 [REDACTED]
17 [REDACTED]
18 [REDACTED]

19 116. Later in the year, Lord reflected on Yahoo's poor approach to information
20 security in response to an inquiry from Verizon regarding security infrastructure at various
21 Yahoo properties:

22 [REDACTED]
23 [REDACTED]
24 [REDACTED]
25 [REDACTED]
26 [REDACTED]
27 [REDACTED]

28 [REDACTED]

1 117. As so many glaring vulnerabilities persisted in Yahoo’s security, it is not at all
2 surprising that, sometime in 2015–2016, Yahoo’s data security was breached yet again. This
3 time, the attack involved “forged cookies,” text files that Yahoo places on user computers
4 when they log in so that users do not need to log in each time they start a new session.
5 Authentication cookies contain information about the user’s session with Yahoo, and these
6 cookies can contain a great deal of information about the user, such as whether that user has
7 already authenticated to the company’s servers.⁴⁰

8 118. The attackers in this case, thought to be the same parties involved in the 2014
9 Breach, were able to forge these authentication cookies, which granted them access to
10 targeted accounts without needing to supply the account’s password. In addition, a forged
11 cookie allowed the attackers to remain logged into the hacked accounts for weeks or
12 indefinitely.

13 119. The Forged Cookie Breach appears to be related to the 2014 Breach because
14 the hackers in the 2014 Breach used some of the data obtained in the 2014 Breach to then
15 forge cookies, help others forge cookies, or use the cookies to gain actual access to specific
16 accounts. Yahoo’s failure to notify its users of the 2014 Breach in a timely manner, as well as
17 its failure to adequately harden its data security after the 2014 Breach directly allowed
18 hackers to continue to infiltrate Yahoo’s databases into 2015 and 2016.

19 120. Once again, there was no response from, or disclosure by, Yahoo.

20 121. Meanwhile, without having disclosed any of these breaches, Yahoo solicited
21 offers to buy the company. Reportedly, Yahoo wanted the offers in by April 19, 2016.⁴¹
22 Yahoo’s failure to disclose the breaches while soliciting offers prevented a mass defection of
23 Yahoo users who might otherwise have left Yahoo after finding out about the breaches, thus
24 allowing Yahoo to artificially inflate its asking price.

25
26
27 ⁴⁰ Krebs, *supra* note 28.

28 ⁴¹ David Goldman, Yahoo is for sale; bidders line up; Marissa Mayer is toast, CNN (Apr. 11, 2016, 10:29 AM), <http://money.cnn.com/2016/04/11/technology/yahoo-sale-marissa-mayer/>.

1 **G. Yahoo Reveals the 2014 Breach Years After It Happened**

2 122. In August 2016, a hacker identifying himself or herself as “peace_of_mind”
3 posted for sale on the dark web the PII from 200 million Yahoo accounts.



10 123. The Chief Intelligence Officer of Arizona cybersecurity company InfoArmor,
11 who first spotted the massive database being offered for sale last August, told the *New York*
12 *Times* in December 2016 that a geographically dispersed hacking group based in Eastern
13 Europe managed to sell copies of the database to three buyers for \$300,000 apiece months
14 before Yahoo disclosed the 2014 Breach.⁴²

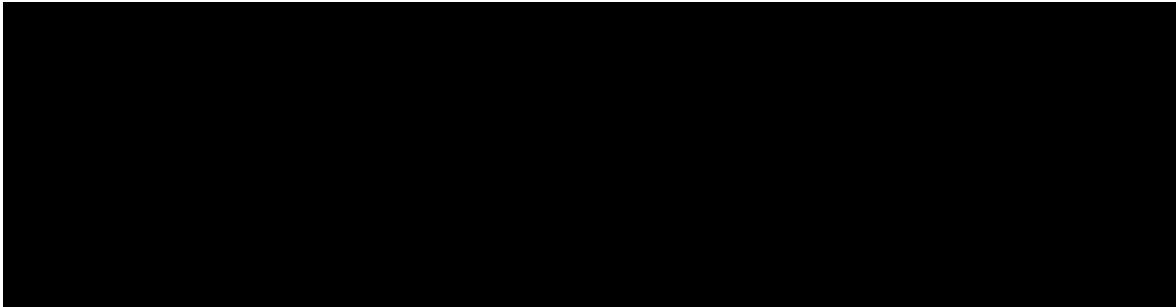
15 124. Yahoo responded to media inquiries about this by noting that it was “‘aware’
16 of the hacker’s claims, but ha[d] not confirmed nor denied the legitimacy of the data” offered
17 for sale.⁴³

18 125. Yahoo’s internal documents contradicted its public statements. In early June
19 of 2016, Bob Lord (CISO) and Ron Bell (GC) communicated about a document titled
20 “Crystal Castle,” which described the Siberia timeline (as shown in paragraph 159, *infra*).
21
22

23 ⁴² Jordan Robertson, Stolen Yahoo Data Includes Government Employee Information,
24 Bloomberg Technology (Dec. 14, 2016, 6:09 PM),
[https://www.bloomberg.com/news/articles/2016-12-15/stolen-yahoo-data-includes-](https://www.bloomberg.com/news/articles/2016-12-15/stolen-yahoo-data-includes-government-employee-information)
25 [government-employee-information](https://www.bloomberg.com/news/articles/2016-12-15/stolen-yahoo-data-includes-government-employee-information); Lisa Vaas, Yahoo breach: your account is selling for
pennies on the dark web, naked security (Dec. 20, 2016),
26 [https://nakedsecurity.sophos.com/2016/12/20/yahoo-breach-your-account-is-selling-for-](https://nakedsecurity.sophos.com/2016/12/20/yahoo-breach-your-account-is-selling-for-pennies-on-the-dark-web/)
[pennies-on-the-dark-web/](https://nakedsecurity.sophos.com/2016/12/20/yahoo-breach-your-account-is-selling-for-pennies-on-the-dark-web/).

27 ⁴³ Joseph Cox, Yahoo ‘Aware’ Hacker Is Advertising 200 Million Supposed Accounts on
Dark Web, MOTHERBOARD (Aug. 1, 2016), [http://motherboard.vice.com/read/yahoo-](http://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web)
28 [supposed-data-breach-200-million-credentials-dark-web](http://motherboard.vice.com/read/yahoo-supposed-data-breach-200-million-credentials-dark-web).

1 The document showed Yahoo was expecting a dump of user credentials at least three months
2 before it publicly announced the 2014 Breach:



8 126. Finally, on September 22, 2016, more than 3 years after the largest breach (the
9 2013 Breach), Yahoo publicly announced that the 2014 Breach had occurred. Yahoo said in a
10 statement that “the account information may have included names, email addresses,
11 telephone numbers, dates of birth, hashed passwords (the vast majority with bcrypt) and, in
12 some cases, encrypted or unencrypted security questions and answers.”⁴⁴ This announcement
13 came just two months after Yahoo announced Verizon’s plan to acquire its operating assets,
14 and just weeks after Yahoo reported to the SEC that it knew of no incidents of unauthorized
15 access of personal data that might adversely affect the potential acquisition.⁴⁵

16 127. Matt Blaze, a
17 cyber security expert and
18 director of the Distributed
19 Systems Lab at the University
20 of Pennsylvania likened the
21 2014 Breach to an “ecological
22 disaster.”



25 ⁴⁴ Yahoo Security Notice September 22, 2016, Yahoo! Help, <https://help.yahoo.com/kb/SLN28092.html> (last visited Apr 9, 2017).

26 ⁴⁵ Kurt R. Hunt, Timing Is Everything in Data Breach Investigations and Disclosures: Yahoo
27 Breach, The National Law Review (Nov. 2, 2016),
28 <http://www.natlawreview.com/article/timing-everything-data-breach-investigations-and-disclosures-yahoo-breach>.

1 128. Yahoo also claimed it did not uncover the 2014 Breach for two years, a claim
2 met with immediate skepticism. A September 23, 2016 *Financial Times* report stated that
3 “Yahoo CEO Marissa Mayer has known that Yahoo was investigating a serious data breach
4 since July, but withheld the information from investors, regulators and acquirer Verizon until
5 this week...”⁴⁶ Only later would Yahoo concede it knew about the 2014 Breach at the time it
6 took place.

7 129. In its 2016 10-K filing with the SEC, Yahoo admitted it had
8 “contemporaneous knowledge” of the 2014 Breach, yet failed to “properly investigate[] and
9 analyze[]” the breach, due in part to “failures in communication, management, inquiry and
10 internal reporting” that led to a “lack of proper comprehension and handling” of the 2014
11 Breach.⁴⁷ Curiously, Yahoo did not disclose in its 10-K that both its CISO and General
12 Counsel were two of the Yahoo executives who possessed that “contemporaneous
13 knowledge.”

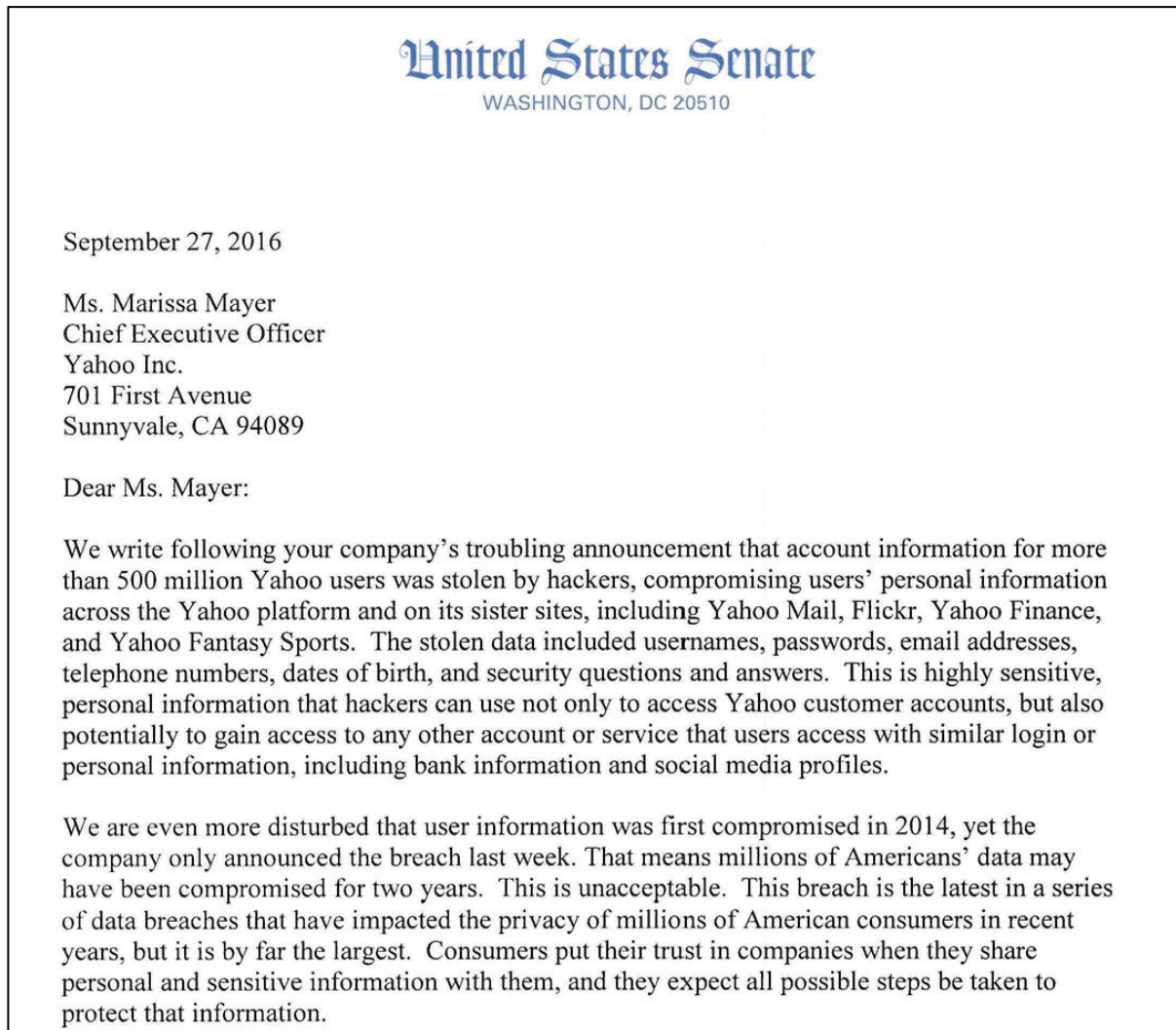
14 130. Yahoo had reason to keep any breach under wraps. It struggled for years to
15 compete with more successful technology giants and has now completed a sale of its
16 operating assets and businesses to Verizon for \$4.48 billion. By intentionally failing to
17 disclose the breach in a timely manner as required by law, Yahoo misled consumers into
18 continuing to sign up for Yahoo services and products, thus providing Yahoo a continuing
19 income stream and a better chance of finalizing a sale of the company to Verizon.

20 131. Yahoo’s lack of timely, legally-mandated disclosure upset several United
21 States senators. On September 27, 2016, after Yahoo’s belated disclosure of the 2014
22 Breach, six senators sent Yahoo CEO Marissa Mayer the below letter, outlining several
23
24
25

26 ⁴⁶ Harriett Taylor, Yahoo CEO Mayer knew about data breach in July: Report, CNBC (Sept.
27 23, 2016, 3:51 PM), <http://www.cnbc.com/2016/09/23/yahoo-ceo-mayer-knew-about-data-breach-in-july-report.html>.

28 ⁴⁷ Yahoo!, Inc. Form 10-K, *supra* note 2, at 47.

1 concerns. Particularly troubling to the senators was Yahoo's failure to notify its users of the
2 2014 Breach sooner:



132. The Plaintiffs and the Class are informed and believe that investigations by the Senate, the Department of Justice, and the Securities and Exchange Commission into Yahoo's failure to disclose the breaches sooner remain ongoing.

H. More Than Three Years After the Fact, Yahoo Finally Acknowledges the 2013 Breach

133. On December 14, 2016, Yahoo finally admitted to the 2013 Breach, though it did not disclose the true scope at the time. Yahoo's Chief Information Security Officer

1 posted the following under an announcement titled “Important Security Information for
2 Yahoo Users”:

3 As we previously disclosed in November, law enforcement provided us
4 with data files that a third party claimed was Yahoo user data. We
5 analyzed this data with the assistance of outside forensic experts and
6 found that it appears to be Yahoo user data. Based on further analysis of
7 this data by the forensic experts, we believe an unauthorized third party, in
8 August 2013, stole data associated with more than one billion user
9 accounts. We have not been able to identify the intrusion associated with
10 this theft.⁴⁸

11 134. In the 2013 Breach, hackers obtained, among other things, class members’
12 Yahoo login (ID), Country Code, Recovery E-Mail (linked with the profile), Date of Birth
13 (DOB), Hash of Password (MD5), and Cell phone number and ZIP code if they were
14 provided by the user for password recovery.⁴⁹ Although Yahoo asserts that the Breaches did
15 not expose credit card data (and there is little reason at this point to give credence to that
16 claim), the Breaches allowed criminals to obtain passwords and login information for Yahoo
17 users’ entire accounts and, thus, obtain the actual content of users’ emails, calendars, and
18 contacts. Consequently, any sensitive data or documents contained in those emails,
19 calendars, and contacts could be compromised—not just credit card numbers, but bank
20 account numbers, Social Security numbers, driver’s license numbers, passport information,
21 birth certificates, deeds, mortgages, and contracts, to name just a few examples.

22 135. Tyler Moffitt, senior threat research analyst at Webroot, said: “All of the data
23 stolen, including emails, passwords and security questions, make a potent package for
24 identify theft. The main email account has links to other online logins and the average user
25 likely has password overlap with multiple accounts.”⁵⁰

26 ⁴⁸ Bob Lord, Important Security Information for Yahoo Users, Yahoo! Tumblr (Dec. 14,
27 2016), <https://yahoo.tumblr.com/post/154479236569/important-security-information-for-yahoo-users>.

28 ⁴⁹ InfoArmor: Yahoo Data Breach Investigation, InfoArmor (Sept. 28, 2016),
<https://www.infoarmor.com/infoarmor-yahoo-data-breach-investigation/>.

⁵⁰ Samuel Gibbs, Security experts: 'No one should have faith in Yahoo at this point', the
guardian (Dec. 15, 2016, 7:29 AM),
<https://www.theguardian.com/technology/2016/dec/15/security-experts-yahoo-hack>.

1 136. Moffitt takes little comfort from Yahoo’s belated efforts to secure user
2 accounts, stating, “These accounts have been compromised for years and the sheer number of
3 them means they have already been a large source of identity theft. No one should have faith
4 in Yahoo at this point.”⁵¹

5 137. One analyst, Jeff Williams, CTO of Contrast Security, characterized the 2013
6 Breach as “the Exxon Valdez of security breaches.”⁵²

7 138. In addition to catching the attention of the international media and several
8 governments, these revelations caused Verizon, which was poised to buy Yahoo’s operating
9 assets and businesses for \$4.83 billion, to demand a \$925 million discount on the purchase
10 price. Ultimately, the parties agreed on a \$350 million price reduction and an adjustment
11 regarding the parties’ respective shares of liability and litigation costs.⁵³

12 **I. Despite All of This, Yahoo *Still* Waits to Notify Users Affected by the Forged**
13 **Cookie Breach**

14 139. Yahoo quietly divulged the Forged Cookie Breach in its 10-Q filing with the
15 SEC filed November 9, 2016.⁵⁴ While filed publicly, the two brief references in the 141-
16 page filing were overshadowed by the ongoing coverage of the 2014, and then 2013,
17 Breaches. Yahoo failed to notify any affected users at that time.

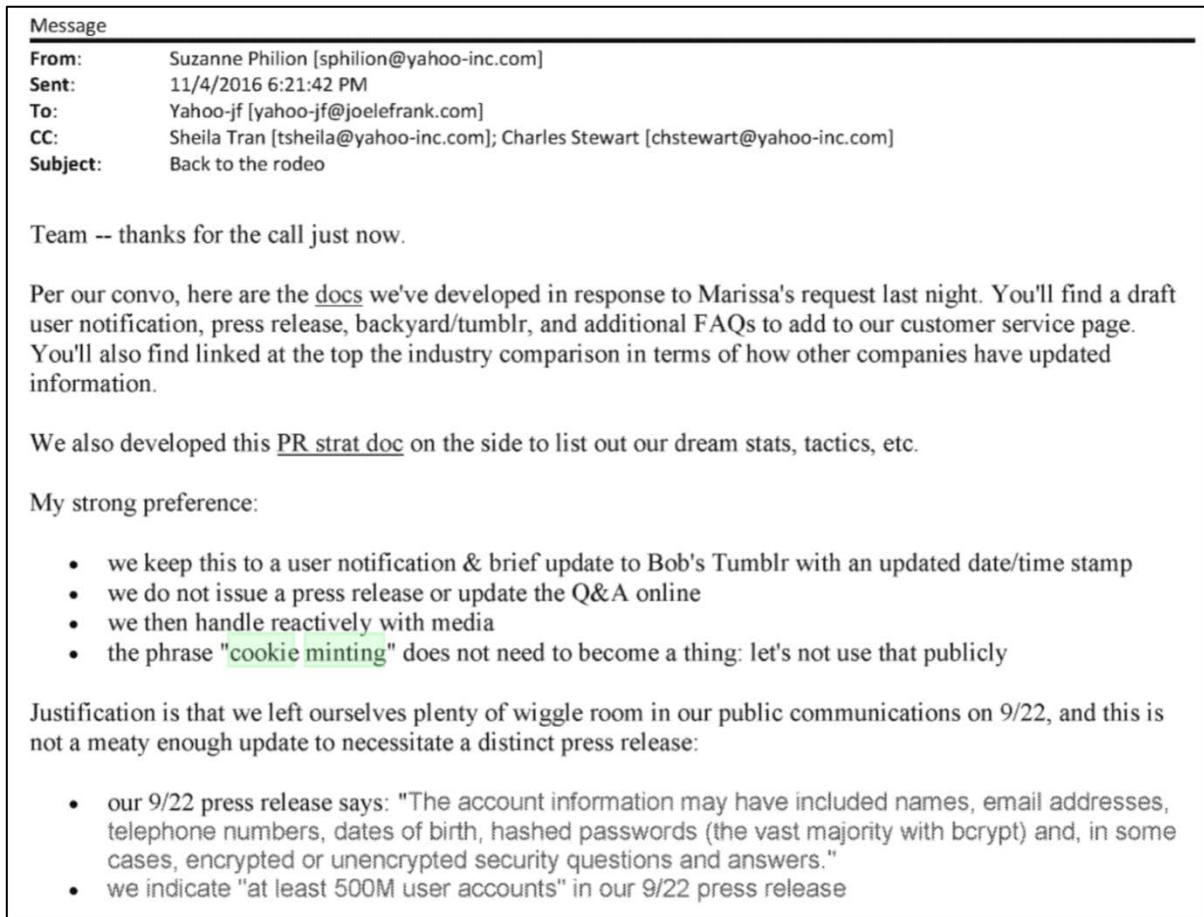
22
23 ⁵¹ *Id.*

24 ⁵² James Rogers, Yahoo hack: The 'Exxon Valdez of security breaches', Fox News (Dec. 15,
2016), [http://www.foxnews.com/tech/2016/12/15/yahoo-hack-exxon-valdez-security-](http://www.foxnews.com/tech/2016/12/15/yahoo-hack-exxon-valdez-security-breaches.html)
25 [breaches.html](http://www.foxnews.com/tech/2016/12/15/yahoo-hack-exxon-valdez-security-breaches.html).

26 ⁵³ Michael Liedtke, Verizon asked for \$925M discount for Yahoo data breaches, The Star
(Mar. 13, 2017), [https://www.thestar.com/business/2017/03/13/verizon-asked-for-925m-](https://www.thestar.com/business/2017/03/13/verizon-asked-for-925m-discount-for-yahoo-data-breaches.html)
27 [discount-for-yahoo-data-breaches.html](https://www.thestar.com/business/2017/03/13/verizon-asked-for-925m-discount-for-yahoo-data-breaches.html).

28 ⁵⁴ Yahoo!, Inc. 2016 Form 10-Q for quarterly period ended Sept. 30, 2016 (Nov. 9, 2016), at
40, 69, [https://investor.yahoo.net/secfiling.cfm?filingID=1193125-16-](https://investor.yahoo.net/secfiling.cfm?filingID=1193125-16-764376&CIK=1011006)
[764376&CIK=1011006](https://investor.yahoo.net/secfiling.cfm?filingID=1193125-16-764376&CIK=1011006).

1 140. In fact, it appears Yahoo's PR strategy for the Forged Cookie Breach was,
2 once again, to wait and see whether anyone would notice the problem:



18 141. Yahoo had drafted notifications pertaining to the Forged Cookie Breach as
19 early as December 15, 2016, but delayed in sending them to affected users.

20 142. Not until February 2017 did Yahoo begin notifying account holders that their
21 email accounts may have been accessed without the need for a password resulting from the
22 use of forged cookies. Yahoo admitted the Forged Cookie Breach was related to the 2014
23 Breach.⁵⁵ Yahoo's notification informed affected users that "a forged cookie may have been
24 used in 2015 or 2016 to access your account."⁵⁶

25

26 ⁵⁵ Mike Snider & Elizabeth Weise, Yahoo notifies users of 'forged cookie' breach, USA
27 Today (Feb. 15, 2017, 3:59 PM),
<http://www.usatoday.com/story/tech/news/2017/02/15/yahoo-notifies-users-forged-cookie-breach/97955438/>.

28 ⁵⁶ *Id.*

1 143. Yahoo claimed that, since discovering the breach, it had “invalidated the
2 forged cookies and hardened [its] systems to secure them against similar attacks.”⁵⁷ Yet,
3 users affected by the Forged Cookie Breach were not notified until many months after Yahoo
4 discovered it.⁵⁸

5 144. Again, data security experts were aghast. One expert, Brian Krebs, saw the
6 Forged Cookie Breach as yet more evidence that Yahoo’s online services are unusable⁵⁹:

7
8 **Q: That sounds pretty bad.**

9 **A: Yeah, that’s about as bad as it gets. It’s yet another reason I’m telling people to run away**
10 **from Yahoo email.**

11 **J. The Full Extent of the Fallout from the Breaches is Not Yet Known**

12 145. Finally, on October 3, 2017, Yahoo/Oath announced that the 2013 Breach had
13 affected every single user account then existing: approximately 3 billion accounts.

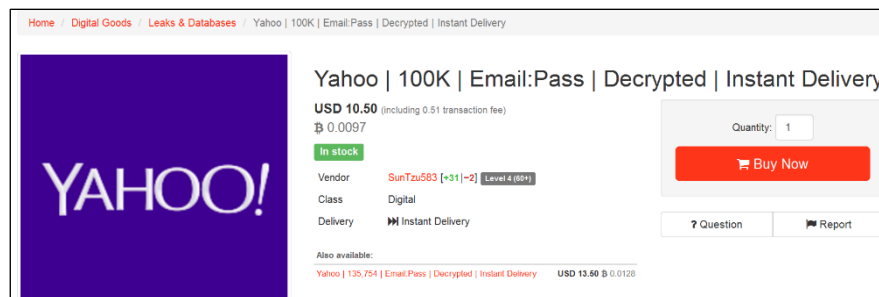
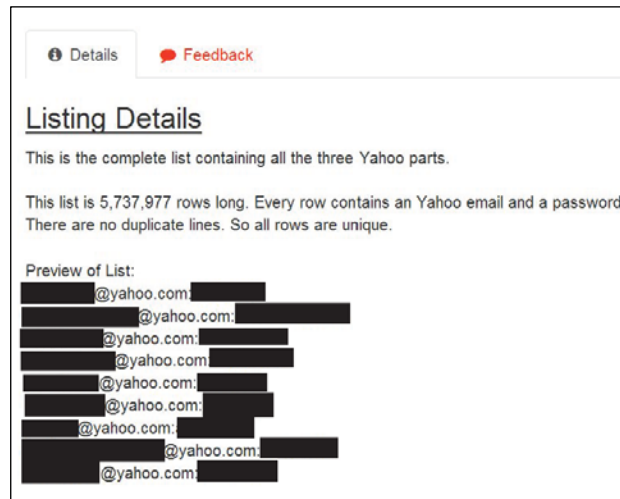
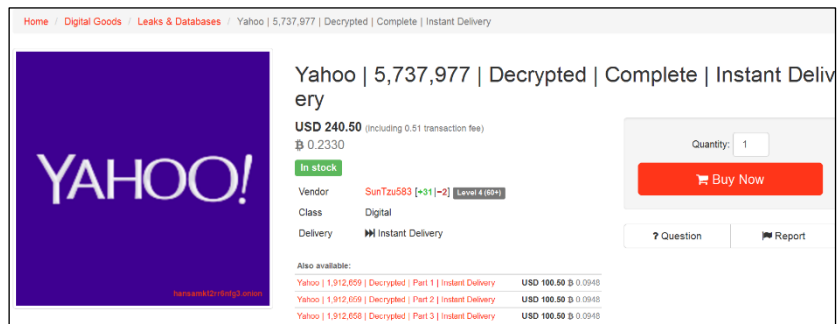
14 146. Yahoo had first been alerted to the information that would lead to this
15 discovery as early as January 31, 2017 but failed to aggressively pursue it until after the
16 Verizon transaction was completed. Even then, it took months for Yahoo/Oath to determine
17 that closer to three billion, not one billion, accounts had been compromised in 2013.

18
19
20
21
22
23
24
25 ⁵⁷ Gareth Halfacree, Yahoo warning users of forged cookie account attacks, bit-tech (Feb. 17,
26 2017), <https://www.bit-tech.net/news/bits/2017/02/17/yahoo-warning-forged-cookies/1>.

27 ⁵⁸ Michelle Castillo, Yahoo's new hack warning comes from a third breach, the company
28 says, CNBC (Feb. 15, 2017, 1:38 PM), <http://www.cnbc.com/2017/02/15/yahoo-sends-new-warning-to-customers-about-data-breach.html>.

⁵⁹ Krebs, *supra* note 28.

1 147. Unfortunately, for the victims of these Yahoo Data Breaches, their stolen
2 information was still for sale on underground hacker forums as late as summer 2017, [REDACTED]
3 [REDACTED] Their PII will be indefinitely
4 available to those who are willing to pay for it as evidenced by the multiple databases for sale
5 online, as shown below:



24 148. Making the situation for Class members even worse, Yahoo does not make it
25 easy to delete user email accounts. Although the process may appear straightforward enough,
26 users have to wait at least 90 days after requesting deletion for it to take effect. And even
27 then, the account often remains active. For example, one user tried to delete his Yahoo
28 account, waited 90 days and on the 91st day checked to see if the account was still active.

1 Unfortunately, and as confirmed by Yahoo, his act of trying to log in to make sure the
2 account was inactive reset the 90-day clock.⁶⁰ Other users have also noted that their accounts
3 remained active long after the 90-day period even though they have not logged in.⁶¹

4 149. The Data Breaches have had internal effects at Yahoo as well. In Yahoo's 10-
5 K filing with the SEC, Yahoo disclosed that an independent committee of Yahoo's Board of
6 Directors had investigated the Data Breaches and determined that Yahoo's information
7 security team knew, at a minimum, about the 2014 Breach and the Forged Cooke Breach as
8 they were happening, but took no real action in the face of that knowledge.⁶²

9 150. With this admission, Yahoo decided it needed a sacrificial lamb, and that
10 person was Ronald Bell, Yahoo's General Counsel. After the independent committee also
11 determined that the Yahoo legal team "had sufficient information to warrant substantial
12 further inquiry in 2014, and they did not sufficiently pursue it," Bell allegedly "resigned"
13 from his position. Yahoo's 10-K notes that "no payments are being made to Mr. Bell in
14 connection with his resignation."⁶³ In other words, he received no severance payment.

15 151. Analysts saw Bell's resignation
16 for what it was—a feeble attempt to create
17 accountability by terminating someone who
18 was not the policy-maker at Yahoo. Yahoo's
19 former head of media, Scott Moore, found the situation "ridiculous."



Scott Moore
@scottm00re



Ridiculous. I know @ronsbell_tech who is a good man and as a lawyer he wasn't in charge of security @Yahoo #ame CYA move
@marissamayer twitter.com/karaswisher/st...
4:25 PM - 1 Mar 2017

16 17 18 19 20 21 22 23 24 25 26 27 28

20 152. In addition, Yahoo's board of directors, "[i]n response to the Independent
21 Committee's findings related to the 2014" breach, elected not to award CEO Marissa Mayer
22 her 2016 cash bonus, and Mayer has supposedly "offered to forgo any equity award in 2017
23 given that the 2014 Security Incident occurred during her tenure."⁶⁴

24
25 ⁶⁰ Zack Whittaker, Deleting your Yahoo email account? Yeah, good luck with that, ZDNet
26 (Feb. 17, 2017, 10:00 PM), <http://www.zdnet.com/article/yahoo-not-deleting-email-accounts-say-users/>.

⁶¹ *Id.*

⁶² See Yahoo!, Inc. Form 10-K, *supra* note 2, at 46-47.

⁶³ *Id.* at 47.

⁶⁴ *Id.*

1 153. The 2014 Breach and Forged Cookie Breach have since been attributed to two
2 Russian FSB agents, a Russian hacker, and a Canadian hacker. A Justice Department
3 spokesperson said of the breaches, “FSB officers used criminal hackers to gain information
4 that clearly ... has intelligence value,” and “the criminal hackers used the opportunity to line
5 their own pockets.”⁶⁵

6 154. It appears that the 2014 Breach began with a “spear phishing” email campaign
7 sent to upper-level Yahoo employees.⁶⁶ One or more of these employees fell for the bait, and
8 Yahoo’s data security was so lax, that this action was enough to hand over the proverbial
9 keys to the kingdom.

10 155. The hackers then managed to infiltrate Yahoo’s UDB, a database containing
11 PII about *all Yahoo users*, including account names, recovery email accounts and phone
12 numbers, password challenge questions and answers, and the account “nonce,” a
13 cryptographic value unique to the targeted victim account. The hackers then downloaded the
14 contents of this database on to their own systems. The hackers also gained access to the
15 AMT, a tool that allowed Yahoo to manage all aspects of its users’ accounts, including
16 making, logging, and tracking changes in the account, such as password changes.⁶⁷

17 156. With these tools, the hackers were able to target all kinds of sources, including
18 specific personal targets and general searches such as credit card verification values (“cvv”
19 numbers), and terms such as “credit card,” “amex,” “visa,” “mastercard,” “gift card,” and
20

21
22 ⁶⁵ Indictment, United States v. Dokuchaev et al. (Feb. 28, 2017), ¶¶ 22-23, 3:17-cr-00103,
23 ECF No. 1; Del Quentin Wilbur & Paresh Dave, Justice Department charges Russian spies,
24 hackers in massive Yahoo breach, Chicago Tribune (Mar. 15, 2017, 3:39 PM),
[http://www.chicagotribune.com/
news/nationworld/ct-russia-yahoo-hacks-20170315-story.html](http://www.chicagotribune.com/news/nationworld/ct-russia-yahoo-hacks-20170315-story.html).

25 ⁶⁶ Indictment, *supra* note 65; *see also* Swati Khandelwal, Yahoo! Hack! How It Took Just
26 One-Click to Execute Biggest Data Breach in History, The Hacker News (Mar. 15, 2017),
<https://thehackernews.com/2017/03/yahoo-data-breach-hack.html>.

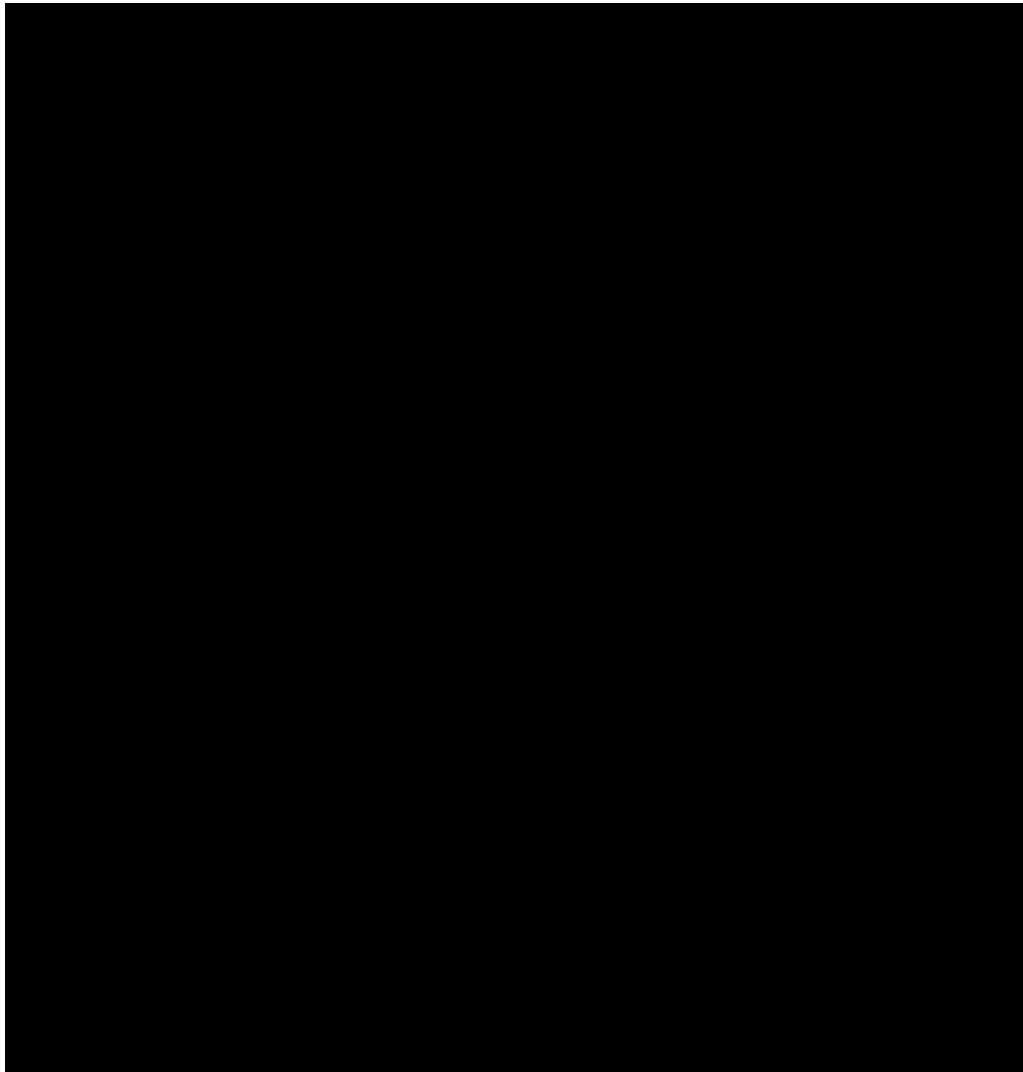
27 ⁶⁷ Indictment, *supra* note 65, ¶¶ 22-33; *see also* Martyn Williams, Inside the Russian hack of
28 Yahoo: How they did it, CSO (March 16, 2017, 4:29 AM),
[http://www.csoonline.com/article/3180762/data-breach/inside-the-russian-hack-of-yahoo-
how-they-did-it.html](http://www.csoonline.com/article/3180762/data-breach/inside-the-russian-hack-of-yahoo-how-they-did-it.html).

1 others.⁶⁸ Through the AMT, they gained direct access to accounts including then-CEO
2 Marissa Mayer's.

3 157. The hackers also used the Yahoo UDB information to compromise related
4 user accounts with cloud-based services like Apple and webmail providers like Google.⁶⁹

5 158. Finally, the hackers were able to use the "nonces" to generate forged cookies
6 so that they could gain continuous access to user accounts without having to re-enter
7 password or other security information.⁷⁰

8 159. In retrospect, it appears the timeline for the Siberia-related intrusions was as
9 follows:



27 ⁶⁸ Indictment, *supra* note 65, ¶¶ 22-33.

28 ⁶⁹ *Id.*

⁷⁰ *Id.*

160. Although Yahoo claims to have plugged the leaks, any fix does not address the fact that Yahoo users' PII is currently in the hands of these hackers, and other miscreants who have obtained Yahoo users' PII by purchase or otherwise. Worse, to date, Yahoo claims it does not—and cannot—determine the root source of the 2013 Breach, in part due to Yahoo's egregious logging procedures.

CLASS ACTION ALLEGATIONS

161. Pursuant to Rule 23(b)(2), (b)(3) and (c)(4) of the Federal Rules of Civil Procedure, Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following classes:

A. The United States Class

All persons who registered for free Yahoo accounts in the United States and whose PII was accessed, compromised, or stolen from Yahoo in the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

B. The Small Business Users Class

All persons who registered for Yahoo Small Business or Aabaco accounts in the United States and whose PII was accessed, compromised, or stolen from Yahoo or Aabaco in the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

C. The Israel Class

All persons who registered for Yahoo accounts in the country of Israel and whose PII was accessed, compromised, or stolen from Yahoo in the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

D. The Paid Users Class

All persons who registered for paid Yahoo accounts (e.g., “ad-free” accounts or other accounts requiring the user to pay money to Yahoo, but excluding Yahoo or Aabaco Small Business Accounts) in the United States and Israel and whose PII was accessed.

1 compromised, or stolen from Yahoo in the 2013 Breach, the 2014
2 Breach, or the Forged Cookie Breach.

3 162. Collectively, all of the classes will be referred to herein as the “Class,” except
4 where otherwise noted in order to differentiate them.

5 163. In addition, Plaintiffs Heines and Dugas bring this action on behalf of a
6 **California subclass** defined as:

7 All persons in California who registered for Yahoo accounts and
8 whose PII was accessed, compromised, or stolen from Yahoo in
9 the 2013 Breach, the 2014 Breach, or the Forged Cookie Breach.

10 164. Excluded from the Class are Defendants and any entities in which any
11 Defendant or their subsidiaries or affiliates have a controlling interest, and Defendants’
12 officers, agents, and employees. Also excluded from the Class are the judge assigned to this
13 action, and any member of the judge’s immediate family.

14 165. **Numerosity:** The members of each Class are so numerous that joinder of all
15 members of any Class would be impracticable. Plaintiffs reasonably believe that Class
16 members number hundreds of millions of people or more in the aggregate and well over
17 1,000 in the smallest of the classes. The names and addresses of Class members are
18 identifiable through documents maintained by Defendants.

19 166. **Commonality and Predominance:** This action involves common questions
20 of law or fact, which predominate over any questions affecting individual Class members,
21 including:

- 22 i. Whether Defendants represented to the Class that they would safeguard
23 Class members’ PII;
24 ii. Whether Defendants owed a legal duty to Plaintiffs and the Class to
25 exercise due care in collecting, storing, and safeguarding their PII;
26 iii. Whether Defendants breached a legal duty to Plaintiffs and the Class to
27 exercise due care in collecting, storing, and safeguarding their PII;
28

- iv. Whether Class members' PII was accessed, compromised, or stolen in the 2013 Breach;
- v. Whether Class members' PII was accessed, compromised, or stolen in the 2014 Breach;
- vi. Whether Class members' PII was accessed, compromised, or stolen in the Forged Cookie Breach;
- vii. Whether Defendants knew about any or all of the Breaches before they were announced to the public and failed to timely notify the public of those Breaches;
- viii. Whether Defendants' conduct violated Cal. Civ. Code § 1750, *et seq.*;
- ix. Whether Defendants' conduct was an unlawful or unfair business practice under Cal. Bus. & Prof. Code § 17200, *et seq.*;
- x. Whether Defendants' conduct violated the Consumer Records Act, Cal. Civ. Code § 1798.80 *et seq.*;
- xi. Whether Defendants' conduct violated the Online Privacy Protection Act, Cal. Bus. & Prof. Code § 22575, *et seq.*;
- xii. Whether Defendants' conduct violated § 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, *et seq.*;
- xiii. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief and restitution; and
- xiv. Whether Plaintiffs and the other Class members are entitled to actual, statutory, or other forms of damages, and other monetary relief.

167. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the members of their respective classes. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

1 168. **Typicality:** Plaintiffs' claims are typical of the claims of the other members of
2 their respective classes because, among other things, Plaintiffs and the other class members
3 were injured through the substantially uniform misconduct by Defendants. Plaintiffs are
4 advancing the same claims and legal theories on behalf of themselves and all other Class
5 members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and
6 those of other Class members arise from the same operative facts and are based on the same
7 legal theories.

8 169. **Adequacy of Representation:** Plaintiffs are adequate representatives of the
9 classes because their interests do not conflict with the interests of the other Class members
10 they seek to represent; they have retained counsel competent and experienced in complex
11 class action litigation and Plaintiffs will prosecute this action vigorously. The Class
12 members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

13 170. **Superiority:** A class action is superior to any other available means for the
14 fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be
15 encountered in the management of this matter as a class action. The damages, harm, or other
16 financial detriment suffered individually by Plaintiffs and the other members of their
17 respective classes are relatively small compared to the burden and expense that would be
18 required to litigate their claims on an individual basis against Defendants, making it
19 impracticable for Class members to individually seek redress for Defendants' wrongful
20 conduct. Even if Class members could afford individual litigation, the court system could
21 not. Individualized litigation would create a potential for inconsistent or contradictory
22 judgments, and increase the delay and expense to all parties and the court system. By
23 contrast, the class action device presents far fewer management difficulties and provides the
24 benefits of single adjudication, economies of scale, and comprehensive supervision by a
25 single court.

26 171. Further, Defendants have acted or refused to act on grounds generally
27 applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief
28

1 with regard to the members of the Class as a whole is appropriate under Rule 23(b)(2) of the
2 Federal Rules of Civil Procedure.

3 172. Likewise, particular issues under Rule 23(c)(4) are appropriate for
4 certification because such claims present only particular, common issues, the resolution of
5 which would advance the disposition of this matter and the parties' interests therein. Such
6 particular issues include, but are not limited to:

- 7 a. Whether Class members' PII was accessed, compromised, or stolen in the
8 2013 Breach;
- 9 b. Whether Class members' PII was accessed, compromised, or stolen in the
10 2014 Breach;
- 11 c. Whether Class members' PII was accessed, compromised, or stolen in the
12 Forged Cookie Breach;
- 13 d. Whether (and when) Defendants knew about any or all of the Breaches before
14 they were announced to the public and whether Defendants failed to timely
15 notify the public of those Breaches;
- 16 e. Whether Defendants' conduct was an unlawful or unfair business practice
17 under Cal. Bus. & Prof. Code § 17200, *et seq.*;
- 18 f. Whether Defendants' representations that they would secure and protect the
19 PII and financial information of Plaintiffs and members of the classes were
20 facts that reasonable persons could be expected to rely upon when deciding
21 whether to use Defendants' services;
- 22 g. Whether Defendants misrepresented the safety of their many systems and
23 services, specifically the security thereof, and their ability to safely store
24 Plaintiffs' and Class members' PII;
- 25 h. Whether Defendants concealed crucial information about their inadequate data
26 security measures from Plaintiffs and the Class;
- 27 i. Whether Defendants failed to comply with their own policies and applicable
28 laws, regulations, and industry standards relating to data security;

- 1 j. Whether Plaintiffs and class members in the Paid User Class are consumers
2 within the meaning of Cal. Civ. Code § 1761(d);
- 3 k. Whether Defendants’ acts, omissions, misrepresentations, and practices were
4 and are likely to deceive consumers;
- 5 l. Whether Defendants knew or should have known that they did not employ
6 reasonable measures to keep Plaintiffs’ and Class members’ PII or financial
7 information secure and prevent the loss or misuse of that information;
- 8 m. Whether Defendants failed to “implement and maintain reasonable security
9 procedures and practices” for Plaintiffs’ and Class members’ PII in violation
10 of California Civil Code section 1798.81.5, subdivision (b) and Section 5 of
11 the FTC Act;
- 12 n. Whether Defendants failed to provide timely notice of the 2013 Breach, the
13 2014 Breach, or the Forged Cookie Breach to Plaintiffs and Class members in
14 violation of California Civil Code § 1798.82;
- 15 o. Whether Defendants’ conduct violated Cal. Bus. & Prof. Code § 22575, *et*
16 *seq.*;
- 17 p. Whether Defendants owed a duty to Plaintiffs and the Class to safeguard their
18 PII and to implement adequate data security measures;
- 19 q. Whether Defendants breached that duty;
- 20 r. Whether Defendants operate a commercial website or online service that
21 collects personally identifiable information through the Internet about
22 individual consumers residing in California, and elsewhere, who use or visit
23 its commercial Web site or online services, within the meaning of California
24 Business and Professions Code § 22575(a);
- 25 s. Whether Defendants failed to adhere to their posted privacy policy concerning
26 the care they would take to safeguard Plaintiffs’ and Class members’ PII in
27 violation of California Business and Professions Code § 22576;
- 28

- 1 t. Whether Defendants negligently and materially failed to adhere to their posted
2 privacy policy with respect to the extent of their disclosure of users' data, in
3 violation of California Business and Professions Code § 22576;
- 4 u. Whether a contract existed between Defendants and Plaintiffs and the Class
5 members, and the terms of that contract;
- 6 v. Whether Defendants breached the contract by having inadequate safeguards;
- 7 w. Whether an implied contract existed between Defendants and Plaintiffs and
8 the Class members and the terms of that implied contract;
- 9 x. Whether Defendants breached the implied contract;
- 10 y. Whether Defendants violated the covenant of good faith and fair dealing
11 implicit in such contract;
- 12 z. Whether Defendants made representations regarding the supposed secure
13 nature of their small business services;
- 14 aa. Whether such representations were false with regard to storing and
15 safeguarding Class members' PII; and
- 16 bb. Whether such representations were material with regard to storing and
17 safeguarding Class members' PII.

18 **CHOICE OF LAW**

19 173. Members of the United States and Paid User Classes, all of whom registered
20 for Yahoo accounts in the United States, were required as a condition of using Yahoo's
21 services to agree to Yahoo's Terms of Service. This was a "clickwrap" agreement where
22 members of the United States and Paid User Classes had to affirmatively accept the Terms.

23 174. Among other provisions, Yahoo's Terms of Service for the United States and
24 Paid User Classes have a forum selection clause and choice of law clause. The pertinent
25 language reads:

26 The Agreement and the relationship between You and the Company **shall**
27 **be governed by the laws of the State of California without regard to**
28 **its conflict of law provisions**, and specifically excluding from application
to this Agreement that law known as the United Nations Convention on

1 the International Sale of Goods. You and the Company agree to submit to
2 the personal jurisdiction of the courts located within the county of Santa
3 Clara, California. The failure of the Company to exercise or enforce any
right or provision of this Agreement shall not constitute a waiver of such
right or provision.

4 175. In accordance with the choice of law provision, Yahoo has stipulated that
5 California common law and statutory law applies to all claims by members of the United
6 States and Paid User Classes as residents of the United States.

7 176. Members of the Small Business Users Class, all of whom registered for
8 Yahoo Small Business or Aabaco accounts in the United States, were also required as a
9 condition of using those services to agree to Terms of Service. This, too, was a “clickwrap”
10 agreement where members of the United States Class had to affirmatively accept the Terms.

11 177. Among other provisions, Aabaco’s Terms of Service have a forum selection
12 clause and choice of law clause. The pertinent language reads:

13 CHOICE OF LAW AND FORUM (LOCATION OF LAWSUIT)

14 The Agreement and the relationship between You and the Company shall
15 be **governed by the laws of the State of California without regard to its**
16 **conflict of law provisions**, and specifically excluding from application to
17 this Agreement that law known as the United Nations Convention on the
18 International Sale of Goods. You and the Company agree to submit to the
personal jurisdiction of the courts located within the county of Santa
Clara, California.

19 178. The members of the Israel Class agreed to Yahoo’s Terms of Service for
20 Israel, which provide that:

21 If you are using...Israeli (il) Services, you are contracting with Yahoo!
22 Inc., 701 First Avenue, Sunnyvale, CA 94089 to provide you with the
23 Services and the **substantive law of the State of California governs the**
24 **interpretation of this ATOS [] and applies to all claims related to it,**
25 **regardless of the conflict of laws principles.** You and Yahoo! Inc.,
26 irrevocably consent to the exclusive jurisdiction and venue of the state
27 courts located in Santa Clara County, California or in the Federal Courts
28 located in the Northern District of California, USA for all disputes arising
out of or relating to this ATOS or arising out of or relating to the
relationship between you and Yahoo regardless of the type of claim.

179. Moreover, because Defendants are headquartered in California and all of their key decisions and operations emanate from California, California law can and should apply to claims relating to the Yahoo Data Breaches, even those made by persons who reside outside of California. In fact, California law should apply to all Plaintiffs' claims, as Defendants' decisions and substandard acts happened in California, and upon information and belief, the Plaintiffs' PII was collected, stored on, and routed through California, and United States-based servers. For the sake of fairness and efficiency, California law should apply to these claims.

CLAIMS ALLEGED ON BEHALF OF ALL CLASSES

First Claim for Relief

Violation of California's Unfair Competition Law ("UCL") – Unlawful Business Practice

(Cal. Bus. & Prof. Code § 17200, *et seq.*)

180. Plaintiffs repeat, reallege, and incorporate by reference the allegations contained in paragraphs 1 through 179 as though fully stated herein.

181. By reason of the conduct alleged herein, Defendants engaged in unlawful practices within the meaning of the UCL. The conduct alleged herein is a "business practice" within the meaning of the UCL.

182. Since November 2015, Aabaco, a wholly owned and controlled subsidiary of Yahoo has been the business entity that Yahoo uses to provide services to small business owners. Aabaco is the successor in interest to the Yahoo Small Business division and is liable as the successor for any wrongdoing by that division before it was dissolved by Yahoo and re-named Aabaco. At all times herein relevant since November 2015, Aabaco has been the alter ego of Yahoo for its small business services.

183. Defendants stored the PII of Plaintiffs and members of their respective Classes in Defendants' electronic and consumer information databases. Defendants falsely represented to Plaintiffs and members of the Classes that their PII databases were secure and that class members' PII would remain private. Defendants misleadingly represented that they

1 had “physical, electronic, and procedural safeguards that comply with federal regulations to
2 protect personal information about you.”⁷¹ Yahoo further misrepresented that it “deploy[ed]
3 industry standard physical, technical, and procedural safeguards that comply with relevant
4 regulations to protect [Class members’] personal information” Defendants knew or should
5 have known they did not employ reasonable, industry standard, and appropriate security
6 measures that complied “with federal regulations” and that would have kept Plaintiffs’ and
7 the other Class members’ PII and financial information secure and prevented the loss or
8 misuse of Plaintiffs’ and the other class members’ PII and financial information. Indeed, at
9 the time of the 2013 Breach, Yahoo’s data encryption protocol, known as MD5, was widely
10 discredited and had been proven, many years prior, easy to break. Additionally, Yahoo’s
11 corporate culture discouraged expenditures that would make their data protection and
12 encryption measures effective.

13 184. Even without these misrepresentations, Plaintiffs and Class members were
14 entitled to assume, and did assume Defendants would take appropriate measures to keep their
15 PII safe. Defendants did not disclose at any time that Plaintiffs’ PII was vulnerable to hackers
16 because Defendants’ data security measures were inadequate and outdated, and Defendants
17 were the only ones in possession of that material information, which they had a duty to
18 disclose. Defendants violated the UCL by misrepresenting, both by affirmative conduct and
19 by omission, the safety of its many systems and services, specifically the security thereof,
20 and their ability to safely store Plaintiffs’ and Class members’ PII. Defendants also violated
21 the UCL by failing to implement reasonable and appropriate security measures or follow
22 industry standards for data security, failing to comply with its own posted privacy policies,
23 and by failing to immediately notify Plaintiffs and the other Class members of the 2014 and
24 Forged Cookie Data Breaches. If Defendants had complied with these legal requirements,
25 Plaintiffs and the other Class members would not have suffered the damages related to the
26 2013 Breach, the 2014 Breach, the Forged Cookie Breach, and consequently from,

27 _____
28 ⁷¹ Security at Yahoo, Yahoo!, <https://policies.yahoo.com/us/en/yahoo/privacy/topics/security/index.htm> (last visited Apr. 8, 2017).

1 Defendants' failure to timely notify Plaintiffs and the Class of the 2014 Breach and Forged
2 Cookie Breach.

3 185. Defendants' acts, omissions, and misrepresentations as alleged herein were
4 unlawful and in violation of, *inter alia*, Cal. Civ. Code § 1798.81.5(b), Section 5(a) of the
5 Federal Trade Commission Act, 15 U.S.C. § 45(a), Cal. Bus. & Prof. Code § 22576 (as a
6 result of Yahoo failing to comply with its own posted privacy policies), and, as to the Paid
7 Users Class, the Consumer Legal Remedies Act, Cal. Civ. Code § 1750 *et seq.*

8 186. Plaintiffs and the Class members suffered injury in fact and lost money or
9 property as the result of Defendants' unlawful business practices.⁷² In particular, Plaintiffs
10 and Class members have suffered from forged credit applications and tax returns; improper
11 or fraudulent charges to their credit/debit card accounts; hacked emails; and other similar
12 harm, all as a result of the Data Breaches. In addition, their PII was taken and is in the hands
13 of those who will use it for their own advantage, or is being sold for value, making it clear
14 that the hacked information is of tangible value. Plaintiffs and Class members have also
15 suffered consequential out of pocket losses for procuring credit freeze or protection services,
16 identity theft monitoring, and other expenses relating to identity theft losses or protective
17 measures. Further, Plaintiffs Neff and Mortensen, and members of the Small Business Class
18 and the Paid Users Class, have lost the benefit of their bargain and purchased services they
19 otherwise would not have, or paid more for supposedly secure services than they would have,
20 had they known the truth regarding Defendants' inadequate data security.

21 187. As a result of Defendants' unlawful business practices, violations of the UCL,
22 Plaintiffs Neff and Mortensen and the members of the Paid Users and Small Business classes
23 are entitled to restitution, disgorgement of wrongfully obtained profits and injunctive relief,
24 and all Plaintiffs and all classes and subclass are entitled to injunctive relief.

25
26
27 ⁷² Plaintiffs recognize that this Court ruled out of pocket expenses and the risk of future harm
28 were not sufficient to confer standing under the UCL, and thus certain named plaintiffs
lacked standing. However, Plaintiffs have included all named representatives in the
"unlawful" and "unfair" UCL causes of action to preserve this issue for appeal.

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26

4
5

6
7

8
9
10
11
12
13
14
15
16

17
18
19
20
21
22

23
24
25
26

28

1 data encryption protocol, known as MD5, was widely discredited and had been proven, many
2 years prior, easy to break. Additionally, Defendants' corporate culture discouraged
3 expenditures that would make their data protection and encryption measures effective.

4 193. Defendants' violated the UCL by misrepresenting, both by affirmative
5 conduct and by omission, the security of their many systems and services, and their ability to
6 safely store Plaintiffs' and Class members' PII. Defendants also violated the UCL by failing
7 to implement and maintain reasonable security procedures and practices appropriate to
8 protect all class members' PII, and by failing to immediately notify Plaintiffs and the other
9 Class members of the Data Breaches. If Defendants followed the industry standards and legal
10 requirements, Plaintiffs and the Class would not have suffered the damages related to the
11 2013 Breach, the 2014 Breach, the Forged Cookie Breach, and consequently from
12 Defendants' failure to timely notify Plaintiffs and the Class of the 2014 Breach and Forged
13 Cookie Breach.

14 194. Defendants also violated their commitment to maintain the confidentiality and
15 security of the PII of Plaintiffs and their respective Classes, and failed to comply with their
16 own policies and applicable laws, regulations, and industry standards relating to data
17 security.

18 195. **Defendants engaged in unfair business practices under the “balancing**
19 **test.”** The harm caused by Defendants' actions and omissions, as described in detail above,
20 greatly outweigh any perceived utility. Indeed, Defendants' failure to follow basic data
21 security protocols and misrepresentations to consumers about Defendants' data security
22 cannot be said to have had any utility at all. Thus, for example, there was no utility in Yahoo
23 continuing to use MD5 encryption years after it had been publicly discredited as a viable
24 encryption protocol. Likewise, there was no utility in Yahoo telling the Class that it had
25 “physical, electronic, and procedural safeguards that comply with federal regulations to
26 protect personal information about you,” and that it deployed “industry standards,” when
27 neither was true. And, there was no utility, other than perhaps to Defendants themselves, in
28 unreasonably waiting to disclose the 2014 Breach and Forged Cookie Breach even though

1 Defendants had contemporaneous knowledge they were happening. All of these actions and
2 omissions were clearly injurious to Plaintiffs and the Class members, directly causing the
3 harms alleged below.

4 196. **Defendants engaged in unfair business practices under the “tethering**
5 **test.”** Defendants’ actions and omissions, as described in detail above, violated fundamental
6 public policies expressed by the California Legislature. *See, e.g.*, Cal. Civ. Code § 1798.1
7 (“The Legislature declares that ... all individuals have a right of privacy in information
8 pertaining to them.... The increasing use of computers ... has greatly magnified the potential
9 risk to individual privacy that can occur from the maintenance of personal information.”);
10 Cal. Civ. Code § 1798.81.5(a) (“It is the intent of the Legislature to ensure that personal
11 information about California residents is protected.”); Cal. Bus. & Prof. Code § 22578 (“It is
12 the intent of the Legislature that this chapter [including the Online Privacy Protection Act] is
13 a matter of statewide concern.”) Defendants’ acts and omissions, and the injuries caused by
14 them are thus “comparable to or the same as a violation of the law ...” *Cel-Tech*
15 *Communications, Inc. v. Los Angeles Cellular Telephone Co.* (1999) 20 Cal.4th 163, 187.

16 197. **Defendants engaged in unfair business practices under the “FTC test.”**
17 The harm caused by Defendants’ actions and omissions, as described in detail above, is
18 substantial in that it affects hundreds of millions of Class members (not to mention many
19 more hundreds of millions of persons who cannot bring claims in this Court) and has caused
20 those persons to suffer actual harms. Such harms include a substantial risk of identity theft,
21 disclosure of Class members’ PII and financial information to third parties without their
22 consent, diminution in value of their PII, consequential out of pocket losses for procuring
23 credit freeze or protection services, identity theft monitoring, and other expenses relating to
24 identity theft losses or protective measures. This harm continues given the fact that Class
25 members’ PII remains in Defendants’ possession, without adequate protection, and is also in
26 the hands of those who obtained it without their consent. Defendants’ actions and omissions
27 violated, *inter alia*, Section 5(a) of the Federal Trade Commission Act, 15 U.S.C. § 45. *See,*
28 *e.g., F.T.C. v. Wyndham Worldwide Corp.*, 10 F. Supp. 3d 602, 613 (D.N.J. 2014), *aff’d*, 799

1 F.3d 236 (3d Cir. 2015); *In re LabMD, Inc.*, FTC Docket No. 9357, FTC File No. 102-3099
2 (July 28, 2016) (failure to employ reasonable and appropriate measures to secure personal
3 information collected violated § 5(a) of FTC Act); *In re BJ's Wholesale Club, Inc.*, FTC
4 Docket No. C-4148, FTC File No. 042-3160 (Sept. 20, 2005) (same); *In re CardSystems*
5 *Solutions, Inc.*, FTC Docket No. C-4168, FTC File No. 052-3148 (Sept. 5, 2006) (same); *see*
6 *also United States v. ChoicePoint, Inc.*, Civil Action No. 1:06-cv-0198-JTC (N.D. Ga. Oct.
7 14, 2009) (“failure to establish and implement, and thereafter maintain, a comprehensive
8 information security program that is reasonably designed to protect the security.
9 confidentiality, and integrity of personal information collected from or about consumers”
10 violates § 5(a) of FTC Act); 15 U.S.C. § 45(n) (defining “unfair acts or practices” as those
11 that “cause[] or [are] likely to cause substantial injury to consumers which [are] not
12 reasonably avoidable by consumers themselves and not outweighed by countervailing
13 benefits to consumers or to competition.”).

14 198. Plaintiffs and the Class members suffered injury in fact and lost money or
15 property as the result of Defendants’ unfair business practices. In particular, Plaintiffs and
16 Class members have suffered from forged credit applications and tax returns; improper or
17 fraudulent charges to their credit/debit card accounts; hacked emails; and other similar harm,
18 all as a result of the Data Breaches. In addition, their PII was taken and is in the hands of
19 those who will use it for their own advantage, or is being sold for value, making it clear that
20 the hacked information is of tangible value. Plaintiffs and Class members have also suffered
21 consequential out of pocket losses for procuring credit freeze or protection services, identity
22 theft monitoring, and other expenses relating to identity theft losses or protective measures.
23 Further, Plaintiffs Neff and Mortensen, and members of the Small Business Class and the
24 Paid Users Class, have lost the benefit of their bargain and purchased services they otherwise
25 would not have, or paid more for supposedly secure services than they would have, had they
26 known the truth regarding Defendants’ inadequate data security.

27 199. As a result of Defendants’ unfair business practices, violations of the UCL,
28 Plaintiffs Neff and Mortensen and the Paid Users and Small Business classes are entitled to

1 restitution, disgorgement of wrongfully obtained profits and injunctive relief, and all
2 Plaintiffs and all classes and subclass are entitled to injunctive relief.

3 **Third Claim for Relief**

4 **Deceit by Concealment — Cal. Civil Code §§ 1709, 1710**

5 200. Plaintiffs repeat, reallege, and incorporate by reference the allegations
6 contained in paragraphs 1 through 179 as though fully stated herein.

7 201. As alleged above, Defendants knew their data security measures were grossly
8 inadequate by, at the absolute latest, 2012. At that time, they were warned by both Mandiant
9 and hackers that their systems were extremely vulnerable to attack, facts Defendants already
10 knew given their previous data breaches and security problems. Defendants also learned
11 about the 2014 Breach while it was happening.

12 202. In response to all of these facts, Defendants chose to do nothing to protect
13 Plaintiffs and the Class or warn them about the security problems and breaches.

14 203. Defendants had an obligation to disclose to all class members that their Yahoo
15 accounts and PII were an easy target for hackers and Defendants were not implementing
16 measures to protect them. Defendants also had a duty to disclose the 2014 Breach when they
17 knew about it.

18 204. Defendants did not do these things. Instead, Defendants willfully deceived
19 Plaintiffs and the Class by concealing the true facts concerning their data security, which
20 Defendants were obligated to, and had a duty to, disclose.

21 205. Had Defendants disclosed the true facts about their dangerously poor data
22 security, Plaintiffs and the Class would have taken measures to protect themselves. Plaintiffs
23 and the Class justifiably relied on Defendants to provide accurate and complete information
24 about Defendants' data security, and Defendants did not.

25 206. Alternatively, given the gaping security holes in Defendants' services and
26 Defendants' refusal to take measures to even detect those holes, much less fix them,
27 Defendants simply should have shut down their current service. Independent of any
28 representations made by Defendants, Plaintiffs and the Class justifiably relied on Defendants

1 to provide a service with at least minimally adequate security measures and justifiably relied
2 on Defendants to disclose facts undermining that reliance.

3 207. Rather than cease offering a clearly unsafe and defective service or disclosing
4 to Plaintiffs and the Class that its services were unsafe and users' PII was exposed to theft on
5 a grand scale, Defendants continued on and willfully suppressed any information relating to
6 the inadequacy of their security.

7 208. These actions are "deceit" under Cal. Civil Code § 1710 in that they are the
8 suppression of a fact, by one who is bound to disclose it, or who gives information of other
9 facts which are likely to mislead for want of communication of that fact.

10 209. As a result of this deceit by Defendants, they are liable under Cal. Civil Code
11 § 1709 for "any damage which [Plaintiffs and the Class] thereby suffer[]."

12 210. As a result of this deceit by Defendants, the PII and financial information of
13 Plaintiffs and the Class were compromised, placing them at a greater risk of identity theft and
14 subjecting them to identity theft, and their PII and financial information was disclosed to
15 third parties without their consent. Plaintiffs and Class members also suffered diminution in
16 value of their PII in that it is now easily available to hackers on the Dark Web. In addition,
17 Plaintiff Neff and the members of the Small Business Users Class and Plaintiff Mortensen
18 and the members of the Paid User Class were damaged to the extent of all or part of the
19 amounts they paid for Defendants' services, because those services were either worth nothing
20 or worth less than was paid for them because of their lack of security. Plaintiffs and the Class
21 have also suffered consequential out of pocket losses for procuring credit freeze or protection
22 services, identity theft monitoring, and other expenses relating to identity theft losses or
23 protective measures.

24 211. Defendants' deceit as alleged herein is fraud under Civil Code § 3294(c)(3) in
25 that it was deceit or concealment of a material fact known to the Defendants conducted with
26 the intent on the part of Defendants of depriving Plaintiffs and the Class of "legal rights or
27 otherwise causing injury." As a result, Plaintiffs and the Class are entitled to punitive
28 damages against Defendants under Civil Code § 3294(a).

1 **Fourth Claim for Relief**

2 **Negligence**

3 212. Plaintiffs repeat, reallege, and incorporate by reference the allegations
4 contained in paragraphs 1 through 179 as though fully stated herein.

5 213. Defendants owed a duty to Plaintiffs and the Class to exercise reasonable care
6 in safeguarding and protecting their PII and keeping it from being compromised, lost, stolen,
7 misused, and or/disclosed to unauthorized parties. This duty included, among other things,
8 designing, maintaining, and testing Defendants' security systems to ensure the PII of
9 Plaintiffs' and the Class was adequately secured and protected, including using encryption
10 technologies. Defendants further had a duty to implement processes that would detect a
11 breach of their security system in a timely manner.

12 214. Defendants knew that the PII of Plaintiffs and the Class was personal and
13 sensitive information that is valuable to identity thieves and other criminals. Defendants also
14 knew of the serious harms that could happen if the PII of Plaintiffs and the Class was
15 wrongfully disclosed, that disclosure was not fixed, or Plaintiffs and the Class were not told
16 about the disclosure in a timely manner.

17 215. By being entrusted by Plaintiffs and the Class to safeguard their PII,
18 Defendants had a special relationship with Plaintiffs and the Class. Plaintiffs and the Class
19 signed up for Defendants' services and agreed to provide their PII with the understanding
20 that Defendants would take appropriate measures to protect it, and would inform Plaintiffs
21 and the Class of any breaches or other security concerns that might call for action by
22 Plaintiffs and the Class. But, Defendants did not. Defendants not only knew their data
23 security was inadequate, they also knew they didn't even have the tools to detect and
24 document intrusions or exfiltration of PII. Defendants are morally culpable, given their
25 repeated security breaches, wholly inadequate safeguards, and refusal to notify Plaintiffs and
26 the Class of breaches or security vulnerabilities,

27 216. Defendants breached their duty to exercise reasonable care in safeguarding
28 and protecting Plaintiffs' and the Class members' PII by failing to adopt, implement, and

1 maintain adequate security measures to safeguard that information, despite repeated failures
2 and intrusions, and allowing unauthorized access to Plaintiffs' and the other Class members'
3 PII.

4 217. Defendants also breached their duty to timely disclose that Plaintiffs' and the
5 other class members' PII had been, or was reasonably believed to have been, stolen or
6 compromised.

7 218. Defendants' failure to comply with industry and federal regulations further
8 evidences Defendants' negligence in failing to exercise reasonable care in safeguarding and
9 protecting Plaintiffs' and the Class members' PII.

10 219. Defendants' breaches of these duties were not merely isolated incidents or
11 small mishaps. Rather, the breaches of the duties set forth above resulted from a long-term
12 company-wide refusal by Defendants to acknowledge and correct serious and ongoing data
13 security problems. Defendants' corporate culture discouraged its own employees from
14 reporting or fixing security issues and encouraged them to look the other way. Defendants
15 also made a company decision not to disclose the 2014 Breach when they knew about it, but
16 rather to sweep it under the rug as long as possible.

17 220. But for Defendants' wrongful and negligent breach of their duties owed to
18 Plaintiff and the Class, their PII would not have been compromised, stolen, and viewed by
19 unauthorized persons. Defendants' negligence was a direct and legal cause of the theft of the
20 PII of Plaintiffs and the Class and all resulting damages.

21 221. The injury and harm suffered by Plaintiffs and the Class members was the
22 reasonably foreseeable result of Defendants' failure to exercise reasonable care in
23 safeguarding and protecting Plaintiff's and the other class members' PII. Defendants knew
24 their systems and technologies for processing and securing the PII of Plaintiffs and the Class
25 had numerous security vulnerabilities.

26 222. As a result of this misconduct by Defendants, the PII and financial
27 information of Plaintiffs and the Class were compromised, placing them at a greater risk of
28 identity theft and subjecting them to identity theft, and their PII and financial information

1 was disclosed to third parties without their consent. Plaintiffs and Class members also
2 suffered diminution in value of their PII in that it is now easily available to hackers on the
3 Dark Web. In addition, Plaintiff Neff and the members of the Small Business Users Class
4 and Plaintiff Mortensen and the members of the Paid User Class were damaged to the extent
5 of all or part of the amounts they paid for Defendants' services, because those services were
6 either worth nothing or worth less than was paid for them because of their lack of security.
7 Plaintiffs and the Class have also suffered consequential out of pocket losses for procuring
8 credit freeze or protection services, identity theft monitoring, and other expenses relating to
9 identity theft losses or protective measures.

10 223. Defendants' misconduct as alleged herein is malice or oppression under Civil
11 Code § 3294(c)(1) and (2) in that it was despicable conduct carried on by Defendants with a
12 willful and conscious disregard of the rights or safety of Plaintiffs and the Class and
13 despicable conduct that has subjected Plaintiffs and the Class to cruel and unjust hardship in
14 conscious disregard of their rights. As a result, Plaintiffs and the Class are entitled to punitive
15 damages against Defendants under Civil Code § 3294(a).

16 **Fifth Claim for Relief**

17 **Breach of Contract**

18 224. Plaintiffs repeat, reallege, and incorporate by reference the allegations
19 contained in paragraphs 1 through 179 as though fully stated herein.

20 225. Yahoo's Privacy Policy is incorporated by reference into its Terms of Service,
21 which forms a binding contract between Yahoo and each user at the time of the creation of an
22 account. The "Security at Yahoo" page is hyperlinked directly from the Yahoo Privacy
23 Policy.

24 226. Yahoo breached the contract with respect to at least the following four
25 provisions of its Privacy Policy.

- 26 • "We are committed to ensuring your information is protected and apply
27 safeguards in accordance with applicable law."
28

- “Yahoo does not rent, sell, or share personal information about you with other people or non-affiliated companies except to provide products or services you’ve requested, when we have your permission, or under [certain inapplicable circumstances].”
- “We limit access to personal information about you to employees who we reasonably believe need to come into contact with that information to provide products or services to you or in order to do their jobs.”
- “We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.”

227. Yahoo further breached the contract with respect to at least the following provisions of the Security at Yahoo page incorporated into the Privacy Policy:

- Promising “a secure user experience”
- “We deploy industry standard physical, technical, and procedural safeguards that comply with relevant regulations to protect your personal information”

228. Aabaco’s Privacy Policy is similarly incorporated by reference into its Terms of Service, forming a binding contract between Aabaco and each user at the time of purchasing any service or product from Aabaco. Aabaco’s Terms of Service for 2009 and 2011-2016 are attached to this First Amended Consolidated Class Action Complaint as Exhibits 16-22. Aabaco’s Privacy Policy further provides that Aabaco shares PII with Yahoo, and “Yahoo’s Privacy Policy governs its use of that information.”

229. Aabaco breached the contract with respect to at least the following three provisions of its Privacy Policy:

- “The Company does not rent, sell, or share Personal Information about You with other people or non-affiliated companies except to provide products or services You've requested, when we have Your permission, or under the following circumstances: ...”
- “We limit access to Personal Information about You to employees, contractors, or service providers who we believe reasonably need to come into

1 contact with that information to provide products or services to You or in
2 order to do their jobs.”

- 3 • “We have physical, electronic, and procedural safeguards that comply with
4 federal regulations to protect Personal Information about You.”

5 230. Defendants breached these provisions of the contracts in that they did not have
6 proper safeguards “in accordance with applicable law” to protect Plaintiffs’ and Class
7 members’ “Personal Information,” including, but not limited to, Section 5(a) of the FTC Act,
8 and did not limit access to that information to the specified individuals or entities.

9 Defendants violated their commitment to maintain the confidentiality and security of the PII
10 of Plaintiffs and the class members, and failed to comply with their own policies and
11 applicable laws, regulations, and industry standards relating to data security.

12 231. The 2013, 2014, and Forged Cookie Data Breaches were a direct and legal
13 cause of the injuries and damages suffered by Plaintiffs and the Class members.

14 232. Both Yahoo’s and Aabaco’s Terms of Service purport to impose a limitation
15 of liability on users who agree to the Terms, in which users agree Defendants will not be
16 liable for indirect, punitive, incidental, special, consequential, or exemplary damages. See,
17 Exhs. 1-6, 16-23. These limitations, by their own terms, do not apply to direct damages.

18 233. Further, to the extent the limitations apply to consequential damages, they are
19 unconscionable under California law.

20 234. California Commercial Code section 2719(b)(3) provides that a contractual
21 limitation of consequential damages is invalid if it is unconscionable. Unconscionability
22 under California law involves both procedural and substantive unconscionability.

23 235. Procedural unconscionability under California law focuses on the factors of
24 surprise and oppression. “Oppression” arises from an inequality of bargaining power which
25 results in no real negotiation and ‘an absence of meaningful choice.’ “Surprise” involves the
26 extent to which the supposedly agreed-upon terms of the bargain are hidden in a prolix
27 printed form drafted by the party seeking to enforce the disputed terms.

1 236. The Yahoo Terms of Service have both. On the issue of surprise, the liability
2 disclaimers appear on pages 8 and 9 of a 12-page “clickwrap” Terms of Service document—
3 in other words, neither at the front or the back, where users are most likely to see them. The
4 Terms of Service itself is a “clickwrap” agreement where the user must scroll through many
5 pages of contract legalese and then check a box on the computer indicating the user has seen
6 and agreed to the Terms. It is fair to say all Plaintiffs and class members would be surprised
7 to find out Defendants disclaimed even the most basic performance characteristics of their
8 products and services.

9 237. On the question of oppression, the Terms of Service themselves are contained
10 in an adhesion contract that allows for no form of negotiation or modification. All of
11 Defendants’ customers must accept the Terms on a take it or leave it basis.

12 238. Substantive unconscionability under California law focuses on the one-
13 sidedness or overly harsh effect of the contract term or clause. Again, the disclaimers by
14 Yahoo are inherently one-sided. Among other things Yahoo’s disclaimers force its customers
15 to agree that Yahoo’s services and software are being provided “as is,” and customers are
16 forced to accept that Yahoo disclaims any warranties of any kind. *See, e.g.*, Exh. 3, pp. 7-8.
17 In other words, Yahoo was providing Plaintiffs and the Class with a product or service and
18 then forcing those people to agree the product or service could be completely useless. “Since
19 a product’s performance forms the fundamental basis for a sales contract, it is patently
20 unreasonable to assume that a buyer would purchase a standardized mass-produced product
21 from an industry seller without any enforceable performance standards.” *A & M Produce Co.*
22 *v. FMC Corp.*, 135 Cal. App. 3d 473, 491 (1982).

23 239. In addition, there is no reasonable commercial justification for such broad
24 disclaimers and limitations on liability. Defendants have obligations under both state and
25 federal law to maintain acceptable levels of data security, so it cannot be commercially
26 reasonable to attempt to evade those legal obligations by way of disclaimers buried in the
27 Terms of Service. Defendants were not selling used products at a yard sale—where an “as is”
28

1 limitation might be commercially appropriate—they are technology giants providing internet
2 services which they advertised as being safe and sophisticated.

3 240. Consequential damages are also a clear and well-understood consequence of
4 a data breach, and allowing Yahoo—an internet titan—to compel individual users who just
5 want to sign up for an email address to disclaim them is a commercially unfair re-allocation
6 of risk.

7 241. Further, the disclaimers are unenforceable under California Civil Code §
8 1668, which prohibits enforcement of contract terms where the contract attempts to “exempt
9 anyone from responsibility for his own fraud, or willful injury to the person or property of
10 another, or violation of law, whether willful or negligent ...”

11 242. Here, to the extent Defendants are seeking to invoke the disclaimers or
12 limitations on liability to avoid responsibility for their violation of several laws, including
13 Section 5 of the FTC Act, the CRA, and the CLRA, among others, they are “against the
14 policy of the law” and cannot be enforced.

15 243. Plaintiffs and the other Class members were harmed as the result of
16 Defendants’ breach of contract terms outlined above, resulting in the 2013, 2014, and Forged
17 Cookie Data Breaches, because their PII and financial information were compromised,
18 placing them at a greater risk of identity theft and subjecting them to identity theft, and their
19 PII and financial information was disclosed to third parties without their consent. Plaintiffs
20 and Class members also suffered diminution in value of their PII in that it is now easily
21 available to hackers on the Dark Web. In addition, Plaintiff Neff and the members of the
22 Small Business Users Class and Plaintiff Mortensen and the members of the Paid User Class
23 were damaged to the extent of all or part of the amounts they paid for Defendants’ services,
24 because those services were either worth nothing or worth less than was paid for them
25 because of their lack of security. Plaintiffs and the Class have also suffered consequential out
26 of pocket losses for procuring credit freeze or protection services, identity theft monitoring,
27 and other expenses relating to identity theft losses or protective measures.

1 **Sixth Claim for Relief**

2 **Breach of Implied Contracts**

3 **(In the Alternative to the Claim for Breach of Express Contract)**

4 244. Plaintiffs repeat, reallege, and incorporate by reference the allegations
5 contained in paragraphs 1 through 179 as though fully stated herein.

6 245. To the extent that Defendants' Terms of Service and Privacy Policies did not
7 form express contracts, the opening of a Yahoo or Aabaco account created implied contracts
8 between Defendants and the user, the terms of which were set forth by the relevant Terms of
9 Service and Privacy Policy (including the Security at Yahoo page hyperlinked therefrom).

10 246. Defendants breached such implied contracts by failing to adhere to the terms
11 of the applicable Policy, as described above in Plaintiffs' Fourth Claim for Relief, ¶¶ 222 -
12 241. Defendants violated their commitment to maintain the confidentiality and security of the
13 PII of Plaintiffs and the Class, and failed to comply with their own policies and applicable
14 laws, regulations, and industry standards relating to data security.

15 247. Plaintiffs and the Class members were harmed as the result of Defendants'
16 breach of the implied contracts because their PII and financial information were
17 compromised, placing them at a greater risk of identity theft and subjecting them to identity
18 theft, and their PII and financial information was disclosed to third parties without their
19 consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it
20 is now easily available to hackers on the Dark Web. In addition, Plaintiff Neff and the
21 members of the Small Business Users Class and Plaintiff Mortensen and the members of the
22 Paid User Class were damaged to the extent of all or part of the amounts they paid for
23 Defendants' services, because those services were either worth nothing or worth less than
24 was paid for them because of their lack of security. Plaintiffs and the Class have also suffered
25 consequential out of pocket losses for procuring credit freeze or protection services, identity
26 theft monitoring, and other expenses relating to identity theft losses or protective measures.
27 The Class members are further damaged as their PII remains in Defendants' possession,
28

1 without adequate protection, and is also in the hands of those who obtained it without their
2 consent.

3 248. This breach of the implied contracts was a direct and legal cause of the
4 injuries and damages to Plaintiffs and members of the Class as described above.

5 **Seventh Claim for Relief**

6 **Breach of the Implied Covenant of Good Faith and Fair Dealing**

7 249. Plaintiffs repeat, reallege, and incorporate by reference the allegations
8 contained in paragraphs 1 through 179 as though fully stated herein.

9 250. Under California law there is an implied covenant of good faith and fair
10 dealing in every contract that neither party will do anything which will injure the right of the
11 other to receive the benefits of the agreement.

12 251. Under the express and implied terms of the agreements entered into between
13 Defendants and Plaintiffs and the Class members, Plaintiffs and the Class members were to
14 benefit through the use of Defendants' services, while those Defendants were supposed to
15 benefit through the limited use of users' data for advertising and product enhancement
16 purposes.

17 252. Defendants exhibited bad faith through their conscious awareness of and
18 deliberate indifference to the risks to Class members' PII, including by (a) using password
19 encryption standards that were long known to be unsafe; (b) taking no serious action in
20 response to past breaches; (c) falling well behind industry standards of cybersecurity; and (d)
21 under-investing in cybersecurity resources despite assurances to its users to the contrary. In
22 doing so, Defendants acted well outside of commercially reasonable norms.

23 253. Defendants, by exposing their users to vastly greater and more harmful
24 exploitation of their PII than they had bargained for, breached the implied covenant of good
25 faith and fair dealing with respect to both the specific contractual terms in Yahoo's Privacy
26 Policy and Aabaco's Privacy Policy and the implied warranties of their contractual
27 relationships with their users.
28

1 254. Plaintiffs and the other Class members were harmed as the result of
2 Defendants' breach of the implied covenant of good faith and fair dealing because their PII
3 and financial information were compromised, placing them at a greater risk of identity theft
4 and their PII and financial information disclosed to third parties without their consent.
5 Plaintiffs and Class members also suffered diminution in value of their PII in that it is now
6 easily available to hackers on the Dark Web. Plaintiff Neff and the members of the Small
7 Business Users Class and Plaintiff Mortensen and the members of the Paid User Class were
8 damaged to the extent of all or part of the amounts they paid for Defendants' services,
9 because those services were either worth nothing or worth less than was paid for them
10 because of their lack of security. Plaintiffs and the Class have also suffered consequential out
11 of pocket losses for procuring credit freeze or protection services, identity theft monitoring,
12 and other expenses relating to identity theft losses or protective measures. The Class
13 members are further damaged as their PII remains Defendants' possession, without adequate
14 protection, and is also in the hands of those who obtained it without their consent.

15 255. Defendants' misconduct as alleged herein is fraud under Civil Code §
16 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants
17 conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of
18 "legal rights or otherwise causing injury." In addition, Defendants' misconduct as alleged
19 herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable
20 conduct carried on by Defendants with a willful and conscious disregard of the rights or
21 safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the
22 Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs
23 and the Class are entitled to punitive damages against Defendants under Civil Code §
24 3294(a).

25 **Eighth Claim for Relief**

26 **Declaratory Relief**

27 256. Plaintiffs repeat, reallege, and incorporate by reference the allegations
28 contained in paragraphs 1 through 179 as though fully stated herein.

1 257. In connection with the active case and controversy between Plaintiffs and
2 Defendants, Plaintiffs seek declaratory relief pursuant to 28 U.S.C. § 2201, declaring that:

3 a. To the extent Plaintiffs' claims for express or implied warranties are
4 covered by Yahoo's Terms of Service, the disclaimer of warranties contained in §
5 19.1 is unconscionable and unenforceable;

6 b. To the extent Plaintiffs' claims are covered by Yahoo's Terms of
7 Service, the limitation of liability in § 20 "resulting from...unauthorized access to
8 ...[users'] data" is unconscionable and unenforceable, or precluded by federal and
9 state law as recognized in § 21;

10 c. To the extent any Plaintiffs' claims for express or implied warranties
11 are covered by Aabaco's Terms of Service, the disclaimer of warranties contained in
12 § 12 is unconscionable and unenforceable;

13 d. To the extent Plaintiffs' claims are covered by Aabaco's Terms of
14 Service, the limitation of liability in § 13 is unconscionable and unenforceable, or
15 precluded by federal and state law; and

16 e. To the extent Plaintiffs' claims are covered by Aabaco's Terms of
17 Service, the one-year limitation contained in § 20 is unconscionable and
18 unenforceable.

19 258. The grounds for unconscionability of the disclaimers and limitations on
20 liability mentioned above are alleged in paragraphs 232-242, *infra*, and are specifically
21 incorporated herein by reference. The shortened one-year statute of limitations clause is
22 unconscionable and unenforceable for the same reasons and also because it benefits only
23 Defendants and deprives Plaintiffs and the Class of their legal rights. *See, e.g., Circuit City*
24 *Stores, Inc. v. Adams*, 279 F.3d 889, 894 (9th Cir. 2002) (one-year limitation on employment
25 claims substantively unconscionable).

1 **ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE SMALL BUSINESS**

2 **USERS CLASS ONLY**

3 **Ninth Claim for Relief**

4 **Violation of California’s Unfair Competition Law (“UCL”) – Fraudulent Business**
5 **Practice**

6 **(Cal. Bus. & Prof. Code § 17200, *et seq.*)**

7 259. Plaintiff Neff repeats, realleges, and incorporates by reference the allegations
8 contained in paragraphs 1 through 179 as though fully stated herein.

9 260. By reason of the conduct alleged herein, Defendants engaged in fraudulent
10 “business practices” within the meaning of the UCL.

11 261. Defendants affirmatively represented to Plaintiff Neff and members of the
12 Small Business Users’ Class that their PII databases were secure and that Class members’ PII
13 would remain private. Defendants engaged in fraudulent acts and business practices by
14 misleadingly representing that they had “physical, electronic, and procedural safeguards that
15 comply with federal regulations to protect personal information about you.” Yahoo further
16 misrepresented that it “deploy[ed] industry standard physical, technical, and procedural
17 safeguards that comply with relevant regulations to protect [Class members’] personal
18 information.” These representations were false, as detailed in the fact section above.

19 262. Defendants not only made affirmative misrepresentations but also made
20 fraudulent omissions by concealing the true facts from Plaintiff Neff and members of the
21 Small Business Users’ Class. Defendants did not disclose to Plaintiff Neff and members of
22 the Small Business Users’ Class that their data security measures were substandard and failed
23 to comply with legal requirements and industry protocols for data security. Defendants also
24 failed to inform Plaintiff Neff and members of the Small Business Users’ Class of the 2014
25 Breach and Forged Cookie Breach in a timely manner despite being required to do so by law.
26 Defendants concealed these material facts from Plaintiff Neff and members of the Small
27 Business Users’ Class even though Defendants had exclusive knowledge of them and
28 Plaintiff Neff and members of the Small Business Users’ Class could not reasonably have

1 been expected to discover them, and even though they contradicted and rendered untrue
2 Defendants' affirmative representations about data security.

3 263. Defendants' representations that they would secure and protect the PII of
4 Plaintiff Neff and members of the Small Business Users' Class were facts that reasonable
5 persons could be expected to rely upon when deciding whether to use Defendants' services.

6 264. Plaintiff Neff and members of the Small Business Users' Class read and relied
7 on these representations in their Terms of Service and the incorporated Privacy Policy in
8 deciding to provide their PII to Defendants. Based on these representations, Plaintiff Neff
9 and members of the Small Business Users' Class were entitled to, and did, assume
10 Defendants would take appropriate measures to keep their PII safe. Defendants did not
11 disclose at any time that Plaintiffs' PII was vulnerable to hackers because Defendants' data
12 security measures were inadequate and outdated.

13 265. Specifically, Plaintiff Neff saw, read, and relied on Defendants'
14 representations and warranties regarding the safety and security of his PII in Yahoo's Privacy
15 Policies and Security at Yahoo (for Yahoo small business users), as more fully alleged
16 herein, and would not have signed up for Defendants' services if he had not believed they
17 were secure.

18 266. Had Plaintiff Neff and members of the Small Business Users' Class known
19 that Defendants' representations about their data security were false, and had Plaintiff Neff
20 and members of the Small Business Users' Class known the material facts Defendants failed
21 to disclose to them about Defendants' substandard data security practices, they would not
22 have provided their PII to Defendants and would not have signed up for Defendants'
23 services.

24 267. Plaintiff Neff and members of the Small Business Users' Class suffered injury
25 in fact and lost money or property as the result of Defendants' fraudulent business practices.
26 In particular, Plaintiff Neff and members of the Small Business Users' Class have suffered
27 from forged credit applications and tax returns; improper or fraudulent charges to their
28 credit/debit card accounts; hacked emails; and other similar harm, all as a result of the Data

1 Breaches. In addition, their PII was taken and is in the hands of those who will use it for their
2 own advantage, or is being sold for value, making it clear that the hacked information is of
3 tangible value. Plaintiff Neff and members of the Small Business Users' Class have also
4 suffered consequential out of pocket losses for procuring credit freeze or protection services,
5 identity theft monitoring, and other expenses relating to identity theft losses or protective
6 measures. Further, Plaintiff Neff and members of the Small Business Users' Class have lost
7 the benefit of their bargain and purchased services they otherwise would not have, or paid
8 more for supposedly secure services than they would have, had they known the truth
9 regarding Defendants' inadequate data security.

10 268. As a result of Defendants' fraudulent business practices, violations of the
11 UCL, Plaintiff Neff and members of the Small Business Users' Class are entitled to
12 restitution, disgorgement of wrongfully obtained profits and injunctive relief.

13 **Tenth Claim for Relief**

14 **Misrepresentation**

15 269. Plaintiff Neff repeats, realleges, and incorporates by reference the allegations
16 contained in paragraphs 1 through 179 as though fully stated herein.

17 270. As outlined above, Defendants made numerous representations, in their
18 advertising and in their Privacy Policies, regarding the supposed secure nature of their data
19 security for their small business services. Such representations were false because
20 Defendants utilized outdated encryption, and failed to disclose that they did not use
21 reasonable, industry-standard means, to safeguard against hacking and theft of customer PII.

22 271. Such representations were material to customers and would-be customers,
23 who reasonably relied on the representations. Plaintiff Neff and other members of the Small
24 Business Users Class would not have agreed to use and pay for the small business services
25 and turn over PII, had they known the truth: that Defendants' services were not as secure as
26 represented or secure by any standard.

27 272. Defendants Yahoo and Aabaco intended that Plaintiff Neff and other Small
28 Business Users Class members rely on their security representations, as they knew no would-

1 be customer would submit PII or entrust an online business to unreasonable security risks. In
2 reliance on these representations and omissions, Plaintiff and the Small Business Users Class
3 contracted with Yahoo and Aabaco for email and web services, and provided their PII, which
4 was ancillary to, but not the subject of, the contracts for services. In addition, Plaintiff Neff
5 and other Small Business Users Class members used Yahoo's and Aabaco's email and web
6 services to complete transactions or send sensitive information including PII. This provision
7 of PII was not part of the contracts with Yahoo and Aabaco.

8 273. Defendants experienced several data breaches prior to the 2013 Breach (and
9 after), had been warned that their encryption was outdated, and rejected the advice from their
10 own security employees or contractors to improve security. Defendants were negligent in
11 their representations.

12 274. As a direct and proximate result of Defendants' wrongful actions and
13 inactions, Plaintiff Neff and the other Small Business Users Class members have been
14 damaged by paying monthly fees to Defendants for something they did not receive: secure
15 small business services.

16 275. As a direct and proximate result of Defendants' negligent, and/or willful,
17 actions and inactions, Plaintiff Neff and the other Small Business Users Class members
18 experienced damage to the PII supplied to Defendants for purposes of their business services
19 contracts, actual identity theft (as in Plaintiff Neff's case) and/or being placed at an
20 imminent, immediate, and continuing increased risk of harm from identity theft and identity
21 fraud, requiring them to take the time and effort to mitigate the actual and potential impact of
22 the Yahoo Data Breaches on their lives.

23 276. As a direct and proximate result of Defendants' negligent, and/or willful,
24 actions and inactions, Plaintiff Neff and the other Small Business Users Class members
25 experienced damage to property that was not the subject of the business services contracts
26 with Defendants Yahoo and Aabaco, including but not limited to the PII contained within
27 private email communications, actual identity theft, damage to their credit, damage to their
28 businesses, and/or being placed at an imminent, immediate, and continuing increased risk of

1 harm from identity theft and identity fraud, requiring them to take the time and effort to
2 mitigate the actual and potential impact of the Yahoo Data Breaches on their lives.

3 277. Defendants' misconduct as alleged herein is fraud under Civil Code §
4 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants
5 conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of
6 "legal rights or otherwise causing injury." In addition, Defendants' misconduct as alleged
7 herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable
8 conduct carried on by Defendants with a willful and conscious disregard of the rights or
9 safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the
10 Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs
11 and the Class are entitled to punitive damages against Defendants under Civil Code §
12 3294(a).

13 **ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE PAID USERS CLASS**

14 **ONLY**

15 **Eleventh Claim for Relief**

16 **Violation of California's Consumer Legal Remedies Act ("CLRA")**

17 **(Cal. Civ. Code § 1750, *et seq.*)**

18 278. Plaintiffs repeat, reallege, and incorporate by reference the allegations
19 contained in paragraphs 1 through 179 as though fully stated herein.

20 279. The CLRA was enacted to protect consumers against unfair and deceptive
21 business practices. It extends to transactions that are intended to result, or which have
22 resulted, in the sale of goods or services to consumers. Yahoo provided services to Plaintiff
23 Mortensen and members of the Paid Users Class within the meaning of Cal. Civ. Code §
24 1761(b), and Yahoo's acts, omissions, representations, and practices as described herein fall
25 within the CLRA.

26 280. Plaintiff Mortensen and the other members of the Paid Users Class are
27 consumers within the meaning of Cal. Civ. Code § 1761(d).
28

1 281. Yahoo’s acts, omissions, misrepresentations, and practices were and are likely
2 to deceive consumers. By misrepresenting the safety and security of its electronic and
3 customer information databases, Yahoo violated the CLRA. Yahoo had exclusive knowledge
4 of undisclosed material facts, namely, that its consumer databases were defective and/or
5 unsecure, and withheld that knowledge from Plaintiff Mortensen and the other members of
6 the Paid Users Class. In addition, Yahoo had contemporaneous knowledge of the 2014 Data
7 Breach and of the Forged Cookie Breach, which it failed to disclose, and withheld from
8 Plaintiff Mortensen and the other members of the Paid Users Class.

9 282. Yahoo’s acts, omissions, misrepresentations, and practices alleged herein
10 violated the following provisions of the CLRA, Civil Code § 1770, which provides, in
11 relevant part, that:

12 (a) The following unfair methods of competition and unfair or deceptive acts or
13 practices undertaken by any person in a transaction intended to result or which results
14 in the sale or lease of goods or services to any consumer are unlawful:

15 (5) Representing that goods or services have sponsorship, approval,
16 characteristics, ingredients, uses, benefits, or quantities which they do not have ...

17 (7) Representing that goods or services are of a particular standard, quality, or
18 grade . . . if they are of another.

19 (14) Representing that a transaction confers or involves rights, remedies, or
20 obligations which it does not have or involve, or which are prohibited by law.

21 (16) Representing that the subject of a transaction has been supplied in accordance
22 with a previous representation when it has not.

23 283. Yahoo stored the PII of Plaintiff Mortensen and the other members of the Paid
24 Users Class in its electronic and consumer information databases. Yahoo represented to
25 Plaintiff Mortensen and the other members of the Paid Users Class that its PII databases were
26 secure and that customers’ PII would remain private. Yahoo engaged in deceptive acts and
27 business practices by providing in its website that “protecting our systems and our users’
28 information is paramount to ensuring Yahoo users enjoy a secure user experience and

1 maintaining our users' trust." Yahoo represented that it has "physical, electronic, and
2 procedural safeguards that comply with federal regulations to protect personal information
3 about you."⁷⁴

4 284. Yahoo knew or should have known that it did not employ reasonable
5 measures to keep the PII or financial information of Plaintiff Mortensen and the other
6 members of the Paid Users Class secure and prevent the loss or misuse of that information. In
7 fact, Yahoo violated its commitment to maintain the confidentiality and security of the PII of
8 Plaintiff Mortensen and the other members of the Paid Users Class, and failed to comply with
9 its own policies as well as applicable laws, regulations, and industry standards relating to
10 data security.

11 285. Yahoo's deceptive acts and business practices induced Plaintiff Mortensen
12 and the other members of the Paid Users Class to use Yahoo's online services, and to provide
13 their PII and financial information. But for these deceptive acts and business practices,
14 Plaintiff Mortensen and the other members of the Paid Users Class would not have provided
15 their PII to Yahoo or signed up for the supposedly secure services.

16 286. Plaintiff Mortensen and the other members of the Paid Users Class were
17 harmed as the result of Yahoo's violations of the CLRA because their PII and financial
18 information were compromised, placing them at a greater risk of identity theft and of their
19 PII and financial information being disclosed to third parties without their consent. Plaintiff
20 Mortensen and the other members of the Paid Users Class also suffered diminution in value
21 of their PII in that it is now easily available to hackers on the Dark Web. Plaintiff Mortensen
22 and the other members of the Paid Users Class have also suffered consequential out of pocket
23 losses for procuring credit freeze or protection services, identity theft monitoring, and other
24 expenses relating to identity theft losses or protective measures.

25
26
27
28 ⁷⁴ See *supra* note 71.

1 287. Plaintiff Mortensen and the other members of the Paid Users Class suffered
2 injury in fact and lost money or property as the result of Yahoo’s failure to secure their PII
3 and financial information.

4 288. As the result of Yahoo’s violation of the CLRA, Plaintiff Mortensen and the
5 other members of the Paid Users Class are entitled to compensatory and exemplary damages,
6 an order enjoining Yahoo from continuing the unlawful practices described herein, a
7 declaration that Yahoo’s conduct violated the CLRA, attorneys’ fees, and the costs of
8 litigation.

9 289. Pursuant to Civil Code § 1782, on September 30, 2016, in the case of *Myers*,
10 *et al.*, v. *Yahoo! Inc.*, Case No. 16-cv-2391, filed in the Southern District of California and
11 consolidated with this action, Plaintiff Paul Dugas, on behalf of themselves and all others
12 similarly situated, notified Yahoo in writing by certified mail of the alleged violations of
13 section 1770 and demanded that the same be corrected. In addition, on April 12, 2017, the
14 named Plaintiffs in the original Consolidated Class Action Complaint served an additional
15 notice under section 1782.

16 **ADDITIONAL CLAIMS ALLEGED ON BEHALF OF THE CALIFORNIA**

17 **SUBCLASS ONLY**

18 **Twelfth Claim for Relief**

19 **Violation of California’s Customer Records Act – Inadequate Security**

20 **(Cal. Civ. Code § 1798.81.5)**

21 290. Plaintiffs Heines and Dugas repeat, reallege, and incorporate by reference the
22 allegations contained in paragraphs 1 through 179 as though fully stated herein.

23 291. Plaintiffs Heines and Dugas bring this claim on behalf of the California
24 Subclass.

25 292. California Civil Code section 1798.80, *et seq.*, known as the “Customer
26 Records Act” (“CRA”) was enacted to “encourage business that own, license, or maintain
27 personal information about Californians to provide reasonable security for that information.”
28 Cal. Civ. Code § 1798.81.5(a)(1).

1 293. Section 1798.81.5, subdivision (b) of the CRA requires any business that
2 “owns, licenses, or maintains personal information about a California resident” to
3 “implement and maintain reasonable security procedures and practices appropriate to the
4 nature of the information,” and “to protect the personal information from unauthorized
5 access, destruction, use, modification, or disclosure.” Section 1798.81.5, subdivision
6 (d)(1)(B) defines “personal information” as including “A username or email address in
7 combination with a password or security question and answer that would permit access to an
8 online account.” “Personal information” also includes an individual’s first name or first
9 initial in combination with a social security number, driver’s license number, account number
10 or credit or debit card number and access code, medical information, or health insurance
11 information. Cal. Civ. Code § 1798.82(h).

12 294. Defendants are businesses that own, license, or maintain personal information
13 about California residents. As alleged in detail above, Defendants failed to “implement and
14 maintain reasonable security procedures and practices appropriate to the nature of the
15 information,” and “to protect the personal information from unauthorized access, destruction,
16 use, modification, or disclosure,” resulting in the 2013 Breach, the 2014 Breach, and the
17 Forged Cookie Breach.

18 295. As the direct and legal result of Defendants’ violation of section 1798.81.5,
19 Plaintiffs Heines and Dugas and the members of the California subclass were harmed
20 because their PII and financial information were compromised, placing them at a greater risk
21 of identity theft and their PII and financial information disclosed to third parties without their
22 consent. Plaintiffs and Class members also suffered diminution in value of their PII in that it
23 is now easily available to hackers on the Dark Web. California members of the Small
24 Business Users Class and members of the Paid User Class were damaged to the extent of all
25 or part of the amounts they paid for Defendants’ services, because those services were either
26 worth nothing or worth less than was paid for them because of their lack of security.
27 Plaintiffs Heines and Dugas and the California subclass have also suffered consequential out
28 of pocket losses for procuring credit freeze or protection services, identity theft monitoring,

1 and other expenses relating to identity theft losses or protective measures. The California
2 subclass members are further damaged as their PII remains Defendants' possession, without
3 adequate protection, and is also in the hands of those who obtained it without their consent.

4 296. Plaintiff Heines and Dugas and the California subclass seek all remedies
5 available under Cal. Civ. Code § 1798.84, including, but not limited to: (a) damages suffered
6 by Plaintiffs and the other class members as alleged above and equitable relief.

7 297. Defendants' misconduct as alleged herein is fraud under Civil Code §
8 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants
9 conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of
10 "legal rights or otherwise causing injury." In addition, Defendants' misconduct as alleged
11 herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable
12 conduct carried on by Defendants with a willful and conscious disregard of the rights or
13 safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the
14 Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs
15 and the Class are entitled to punitive damages against Defendants under Civil Code §
16 3294(a).

17 **Thirteenth Claim for Relief**

18 **Violation of California's Customer Records Act – Delayed Notification**

19 **(Cal. Civ. Code § 1798.82)**

20 298. Plaintiffs Heines and Dugas repeat, reallege, and incorporate by reference the
21 allegations contained in paragraphs 1 through 179 as though fully stated herein.

22 299. Plaintiffs Heines and Dugas bring this claim on behalf of the California
23 Subclass.

24 300. Section 1798.82 of the California Civil Code requires any "person or business
25 that conducts business in California, and that owns or licenses computerized data that
26 includes personal information" to "disclose any breach of the security of the system
27 following discovery or notification of the breach in the security of the data to any resident of
28 California whose unencrypted personal information was, or is reasonably believed to have

1 been, acquired by an unauthorized person.” Under section 1798.82, the disclosure “shall be
2 made in the most expedient time possible and without unreasonable delay ...”

3 301. The statute further provides: “Any person or business that maintains
4 computerized data that includes personal information that the person or business does not
5 own shall notify the owner or licensee of the information of any breach of the security of the
6 data immediately following discovery, if the personal information was, or is reasonably
7 believed to have been, acquired by an unauthorized person.” Cal. Civ. Code § 1798.82(b).

8 302. Any person or business that is required to issue a security breach notification
9 under the CRA shall meet all of the following requirements:

- 10 (1) The security breach notification shall be written in plain language;
11 (2) The security breach notification shall include, at a minimum, the following
12 information:

13 (A) The name and contact information of the reporting person or
14 business subject to this section;

15 (B) A list of the types of personal information that were or are
16 reasonably believed to have been the subject of a breach;

17 (C) If the information is possible to determine at the time the notice is
18 provided, then any of the following:

19 (i) the date of the breach,

20 (ii) the estimated date of the breach, or

21 (iii) the date range within which the breach occurred. The
22 notification shall also include the date of the notice;

23 (D) Whether notification was delayed as a result of a law enforcement
24 investigation, if that information is possible to determine at the time
25 the notice is provided;

26 (E) A general description of the breach incident, if that information is
27 possible to determine at the time the notice is provided; and
28

1 (F) The toll-free telephone numbers and addresses of the major credit
2 reporting agencies if the breach exposed a social security number or a
3 driver's license or California identification card number.

4 303. The Data Breaches described previously in this First Amended Consolidated
5 Class Action Complaint each constituted a "breach of the security system" of Defendants.

6 304. As alleged above, Defendants unreasonably delayed informing members of
7 the California subclass about the 2013 Breach, 2014 Breach, and the Forged Cookies Breach,
8 affecting the confidential and non-public PII and financial information of Plaintiffs Heines
9 and Dugas and the members of the California subclass, after Defendants knew each of those
10 Data Breaches had occurred.

11 305. Defendants failed to disclose to Plaintiffs Heines and Dugas and the members
12 of the California subclass, without unreasonable delay and in the most expedient time
13 possible, the breach of security of their unencrypted, or not properly and securely encrypted,
14 PII and financial information when Defendants knew or reasonably believed such
15 information had been compromised.

16 306. Yahoo's ongoing business interests, and in particular its impending sale to
17 Verizon, gave Defendants incentive to conceal the 2013, 2014, and Forged Cookie Data
18 Breaches from the public to ensure continued revenue and a high stock price for the sale.

19 307. Upon information and belief, no law enforcement agency instructed
20 Defendants that notification to Plaintiffs Heines and Dugas and the members of the
21 California subclass would impede its investigation.

22 308. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiffs
23 Heines and Dugas and the members of the California subclass were deprived of prompt
24 notice of the 2013, 2014, and Forged Cookie Breaches and were thus prevented from taking
25 appropriate protective measures, such as changing their password, canceling their account,
26 securing identity theft protection, or requesting a credit freeze. These measures would have
27 prevented some or all of the damages suffered by Plaintiffs Heines and Dugas and the
28

1 members of the California subclass because their stolen information would not have any
2 value to identity thieves.

3 309. For example, had Defendants provided Plaintiff Heines with prompt notice of
4 the 2014 Breach, rather than two years later, she could have changed her security information
5 and likely could have prevented the theft of her monthly Social Security Disability payment
6 in 2015 and its unauthorized use to buy gift cards.

7 310. As a result of Defendants' violation of Cal. Civ. Code § 1798.82, Plaintiffs
8 Heines and Dugas and the members of the California subclass suffered incrementally
9 increased damages separate and distinct from those simply caused by the breaches
10 themselves.

11 311. Plaintiffs Heines and Dugas and the members of the California subclass seek
12 all remedies available under Cal. Civ. Code § 1798.84, including, but not limited to: (a)
13 damages suffered by Plaintiffs and the other class members as alleged above and equitable
14 relief.

15 312. Defendants' misconduct as alleged herein is fraud under Civil Code §
16 3294(c)(3) in that it was deceit or concealment of a material fact known to the Defendants
17 conducted with the intent on the part of Defendants of depriving Plaintiffs and the Class of
18 "legal rights or otherwise causing injury." In addition, Defendants' misconduct as alleged
19 herein is malice or oppression under Civil Code § 3294(c)(1) and (2) in that it was despicable
20 conduct carried on by Defendants with a willful and conscious disregard of the rights or
21 safety of Plaintiffs and the Class and despicable conduct that has subjected Plaintiffs and the
22 Class to cruel and unjust hardship in conscious disregard of their rights. As a result, Plaintiffs
23 and the Class are entitled to punitive damages against Defendants under Civil Code §
24 3294(a).

1 **PRAYER FOR RELIEF**

2 WHEREFORE, Plaintiffs, individually and on behalf of the other Class members,
3 respectfully requests that this Court enter an Order:

4 (a) Certifying the United States Class and California Subclass, Small Business
5 Users' Class, Israel Class, and Paid Users Class, and appointing Plaintiffs as Class
6 Representatives;

7 (b) Finding that Defendants' conduct was negligent, deceptive, unfair, and
8 unlawful as alleged herein;

9 (c) Enjoining Defendants from engaging in further negligent, deceptive, unfair,
10 and unlawful business practices alleged herein;

11 (d) Awarding Plaintiffs and the Class members actual, compensatory, and
12 consequential damages;

13 (e) Awarding Plaintiffs and the Class members statutory damages and penalties,
14 as allowed by law;

15 (f) Awarding Plaintiffs and the Class members restitution and disgorgement;

16 (g) Requiring Defendants to provide appropriate credit monitoring services to
17 Plaintiffs and the other class members;

18 (h) Awarding Plaintiffs and the Class members punitive damages for the Third,
19 Fourth, Seventh, and Tenth through Thirteenth claims for relief;

20 (i) Awarding Plaintiffs and the Class members pre-judgment and post-judgment
21 interest;

22 (j) Awarding Plaintiffs and the Class members reasonable attorneys' fees costs
23 and expenses, and;

24 (k) Granting such other relief as the Court deems just and proper.
25
26
27
28

- 1
- 2
- 3
- 4
- 5
- 6
- 7
- 8
- 9
- 10
- 11
- 12
- 13
- 14
- 15
- 16
- 17
- 18
- 19
- 20
- 21
- 22
- 23
- 24
- 25
- 26
- 27
- 28

Dated: December 15, 2017

/s/ John A. Yanchunis
JOHN A. YANCHUNIS

On behalf of Plaintiffs' Lead Counsel
and Executive Committee